HAAGA-HELIA
ammattikorkeakoulu

Anonyymi asiointi verkossa

Jani Rossi

Opinnäytetyö
Tietojenkäsittelyn
koulutusohjelma
2015

HAAGA-HELIA
ammattikorkeakoulu

Tiivistelmä

23.04.2015

Tekijä(t)
Jani Rossi

Koulutusohjelma
Tietojenkäsittelyn koulutusohjelma

Opinnäytetyön otsikko
Anonyymi asiointi verkossa

Sivu- ja liitesivumäärä
58 + 6

Opinnäytetyön otsikko englanniksi
Online anonymity and home users

Tässä opinnäytetyössä tutustutaan verkkoanonymiteettiin ja sitä sivuaviin aihealueisiin tavallisten kotikäyttäjien näkökulmasta. Verkkoanonymiteetin katsotaan toteutuvan silloin, kun käyttäjiin ei suoranaisesti pystytä linkittämään mitään yksilöivää informaatiota, josta mahdollisesti saataisiin selville näiden henkilöllisyys. Tämän turvin käyttäjät pystyvät asioimaan verkossa nimettömästi ja vaihtamaan mielipiteitään asioista, joista puhuminen julkisesti saattaa olla vaikeaa ja toisinaan jopa paheksuttavaa. Verkkoanonymiteetti edistää ennen kaikkea sananvapauden toteutumista, minkä katsotaan ainakin länsimaissa olevan kaikkien perusoikeus. Valitettavasti kaikki verkkoanonymiteetin lieveilmiöt eivät kuitenkaan ole positiivia, vaan nimettömyyden turvin myös rikollisen toiminnan harjoittaminen ja muihin käyttäjiin kohdistuva häiriköinti on mahdollista.

Projektin perimmäisenä tarkoituksena on lähteä selvittämään, mitä verkkoanonymiteetti on, millaisia vaikutuksia sillä on käyttäjiin ja millä tavoin käyttäjät pystyvät vaikuttamaan omaan yksityisyyteensä. Projektin hallinnallisista syistä työssä keskitytään yksinomaan pc-puoleen ja ennen kaikkea Windows-käyttäjiin. Näin ollen työn ulkopuolelle jäävät mobiililaitteiden lisäksi myös muut käyttöjärjestelmät.

Työn ensimmäinen puolisko muodostuu teoriataustasta, jossa käsitellään verkkoanonymiteetin hyötyjen ja haittojen lisäksi yksityisyyteen liittyvää lainsäädäntöä sekä verkkomainontaa ja käyttäjiin kohdistuvaa tietojenkeruuta. Teoriataustan tukena käytetään tieteellisten artikkelien ja tutkielmien lisäksi verkkolehtien uutisia ja blogikirjoituksia. Työn jälkimmäisellä puoliskolla tutustutaan muun muassa Tor ja Freenet nimisten ohjelmistojen käyttöönottoon ja ominaisuuksiin, verkkoselainten asetusmäärittelyihin sekä muihin menetelmiin, joilla pystytään kohentamaan yksityisyyden suojaa.

Projektin tuotoksena syntyy kirjallisuuskatsaus, joka tarjoaa tiiviin tietopaketin verkkoanonymiteetin nykytilasta ja menetelmistä, joilla pystytään hyödyntämään sen tarjoama koko potentiaali. Yhteenvedosta ilmenee, ettei verkkoanonymiteetin vaikutuksia pystytä vertailemaan täysin yhdenmukaisesti, koska siitä koituvat hyödyt ja haitat saattavat vaikuttaa yksilöihin hyvin eri tavoin. Verkossa asioidessa kannattaa siis tiedostaa anonymiteetin tarjoamat mahdollisuudet, mutta samalla tulee varautua myös negatiivisempiin lieveilmiöihin.

Asiasanat
anonymiteetti, verkkoanonymiteetti, yksityisyys, Tor, Freenet

HAAGA-HELIA
University of Applied Sciences

Abstract

23.04.2015

Author(s)
Jani Rossi

Degree programme
Business Information Technology

Report/thesis title
Online anonymity and home users

Number of pages and appendix pages
58 + 6

The objective of this thesis is to further clarify the term online anonymity and ponder how it affects regular users and their everyday user behaviour patterns. In addition, the aim is also to explore methods and possibilities that allow users to secure their privacy on the Internet. The scope of the thesis had to be narrowed down so it was decided to focus on the PC side and particularly on Windows users. Therefore, mobile devices and other operating systems were beyond the scope of the thesis.

Online anonymity is defined to be fulfilled when users cannot be linked directly to any information which could reveal their true identity. This allows users to browse the web anonymously and exchange views on matters which cannot be discussed in public. Above all, online anonymity promotes the freedom of speech, which is considered to be a fundamental right, at least, in the West. Unfortunately, online anonymity also has its downside and it makes acts such as cyberbullying, and drug trafficking possible.

There has been included an extensive theoretical part which deals with the advantages and demerits of online anonymity, privacy-related legislation, in addition to online advertising and data collecting. The statements in the theoretical part were supported by scientific articles, blog posts and news releases. The second half of the thesis study software solutions which are capable of enhancing user anonymity, such as Tor. This section also contains tips and information about simpler solutions like how users can achieve better privacy by configuring browser settings.

The project resulted in a compact guidebook, which offers information about the current state of online anonymity and how it can be utilized to unlock its full potential. The summary concluded that it is not possible to compare the pros and cons equally, because the benefits and burdens may affect individuals very differently. Therefore it is important to fully understand what online anonymity has to offer and how it can affect web browsing.

Keywords
anonymity, online anonymity, privacy, Tor, Freenet

Sisällys

1 Johdanto

Yksityisyys. Internet. Yksityisyys internetissä. Sanapari, joka herättää meissä jokaisessa tuntemuksia ja mielipiteitä. Tietomurroista ja henkilötietoihin kohdistuneista väärinkäytöksistä uutisoidaan jatkuvasti, mikä on puolestaan herättänyt kiivasta keskustelua, niin mediassa kuin erinäisillä internetin keskustelupalstoillakin.

1.1 Tutkimuksen tavoitteet, rakenne ja rajaus

Tämän opinnäytetyön pääasiallisena tavoitteena on tutkia ja kartoittaa menetelmiä, joilla kotikäyttäjät pystyvät parantamaan identiteettinsä suojaa Internetissä asioidessaan. Samalla pohditaan anonyymiyden todellista tarpeellisuutta sekä vertaillaan siitä koituvia hyötyjä ja haittoja. Tämän lisäksi pyrkimyksenä on luoda kattava, kuitenkin helpposelkoinen dokumentointi, jonka avulla kotikäyttäjät pystyvät tutustumaan siinä esille tuotuihin menetelmiin ja ohjelmistoihin.

Työn rakenne tulee noudattamaan perinteistä vetoketjumallia, jossa asiakokonaisuudet käsitellään yksi kerrallaan. Jokainen kappale tulee käsittelemään omaa erillistä aihealuettaan ja tietyissä osioissa teorianosuuksien lisäksi käsiteltyä aihetta havainnollistetaan asiayhteyteen sopivilla tavoilla, esimerkiksi TORin käyttöönotto vaihe vaiheelta.

Mobiililaitteiden käyttö on yleistynyt räjähdysmäisesti kotitalouksissa viimeisten vuosien aikana, mutta vaikka niiden käyttöön pätevät lähestulkoon samat perusperiaatteet kuin tavallisten tietokoneidenkin, niin siitä huolimatta mobiililaitteiden käsittely ja niihin liittyvä soveltaminen tullaan rajaamaan tämän työn ulkopuolelle ja keskitytään yksinomaan Windows-pohjaisten koneiden käyttöön. Windows-painotteinen lähestymistapa on luontevin vaihtoehto, koska suurin osa tavallisten kotikäyttäjien tietokoneista pyörii jonkin Windows-käyttöjärjestelmän päällä ja näin ollen työn tuloksista tulee hyötymään mahdollisimman moni. (Netmarketshare 2014.)

Jokaista aihealueita pyritään tutkimaan ennen kaikkea suomalaisten käyttäjien näkökulmasta. Tästä johtuen esimerkiksi lainsäädäntöä käsittelevässä kappaleessa ei perehdytä USA:han tai siellä meneillään oleviin lakialoitteisiin kovinkaan tarkasti, vaikka ne saattavat tulevaisuudessa kuitenkin vaikuttaa myös suomalaisten käyttäjien arkeen.

Käsitelista

Opinnäytetyön sisältö pyritään pitämään lähtökohtaisesti hyvin selkokielisenä ja helppolukuisena, mutta väistämätön tosiasia on, että työssä tullaan käyttämään sellaisia käsitteitä, joille ei välttämättä löydy loogisia suomenkielisiä vastineita tai ne ovat muuten vaikeasti ymmärrettävissä.

Anonyymi verkko on oma erillinen kokonaisuutensa, jonka avulla käyttäjät pystyvät pitäytymään nimettöminä muiden käyttäjien keskuudessa. Tämän lisäksi anonyymit verkot mahdollistavat pääsyn käsiksi sivustoihin tai dataan, jotka eivät ole käyttäjien ulottuvilla normaaleja Internetin selaustapoja käyttämällä, vaan niiden käyttö vaatii oman erillisen ohjelmistonsa.

Deep webin määritelmästä on toisistaan hieman eriäviä näkemyksiä, mutta yleisesti ottaen sen alaisuuteen katsotaan kuuluvan kaikki sellainen informaatio, joka on tavallisimpien hakukoneiden ulottumattomissa.

Eväste (cookie) on käyttäjän tietokoneelle tallentuva tiedosto, joka sisältää informaatio käyttäjästä ja tämän toiminnasta.

Haktivisti(t) on henkilö tai ryhmä, joka pyrkii saamaan kuuluvuutta omille poliittisille näkemyksilleen verkossa. Käytännössä tämä tapahtuu kaappaamalla yritysten ja järjestöjen verkkosivustoja tai poliittisten vaikuttajien sosiaalisen median käyttäjätilejä, joiden kautta kyseinen taho ryhtyy levittämään omaa sanomaansa.

IP-osoite on uniikki numerosarja, joka yksilöi Internetiin yhteydessä olevan tietokoneen tai muun tietoteknisen laitteen.

Solmu (node) on nimitys, jota käytetään laitteista ja ohjelmistoista, jotka ovat osa tietoverkkoa.

Välityspalvelin on palvelin tai ohjelmisto tietokoneella, jonka tarkoitus on reitittää yhteydet käyttäjän tietokoneen (tai laitteen) ja kohdepalvelimen välillä.

2 Anonymiteetti

Teknologia on ottanut valtavia harppauksia viimeisten parin vuosikymmenen aikana. Tämän seurauksena myös käyttämämme laitteet ja palvelut ovat kehittyneet valtavasti, mikä puolestaan on antanut meille mahdollisuuden hoitaa tiettyjä asioita huomattavasti nopeammin ja vaivattomammin kuin aikaisemmin.

Vaikka arkipäiväiset askareemme ovat helpottuneet, niin tilalle on ilmaantunut uudenlaisia huolia. Jokapäiväisessä käytössämme olevat laitteet sekä niiden ohjelmistot ja sovellukset keräävät meistä jatkuvasti henkilökohtaista dataa, analysoivat hakukonesyötteitämme ja tallentavat paikannustietojamme. Vaikka tämä onkin erittäin kärjistetty ilmaus teknologian nykytilanteesta, on sanomattakin selvää, että yksityisyytemme on jatkuvasti uhattuna verkossa asioidessamme. Kaikeksi onneksi on kuitenkin olemassa menetelmiä ja tapoja, joilla kykenemme varjelemaan yksityisyyttämme ja ehkäisemään henkilökohtaisten tietojemme joutumista väärien tahojen käsiin internetissä asioidessamme. Pystymme siis liikkumaan verkossa nimettömästi, anonyymisti.

Anonyymius ja anonymiteetti ovat termejä, jotka nykypäivänä assosioidaan ehkä turhankin helposti rikollisuuteen ja hämäräperäiseen toimintaan, mihin ehkä suurimpana vaikuttajana on ollut Anonymous – ryhmänä tunnetun haktivistikollektiivin saama medianäkyvyys. (Hacker News 2014.)

Tämän luvun tarkoituksena on selventää, mitä anonyymius ja anonyymiteetti käytännössä tarkoittavat, pohtia niiden tarpeellisuutta kotikäyttäjän näkökulmasta sekä tuoda esille aihealueeseen liittyviä ongelmakohtia.

2.1 Anonyymiteetin yleinen määritelmä

Nykypäivänä sana anonyymi liitetään automaattisesti Internetiin tai sen käyttöön. Tämä ei sinänsä ole mitenkään kummallista, koska onhan Internet nykypäivän infrastruktuurin yksi tärkeimpiä kulmakiviä, jonka olemassaoloa emme sen koomin edes ajattele. Anonyymius ei kuitenkaan ole mikään internetin jälkituotoksena syntynyt konsepti, vaan käsite on ollut olemassa jo vuosisatojen ajan. Anonyymi sana on peräisin kreikan kielestä (ἀνωνυμία, anonymia), joka vapaasti käännettynä tarkoittaa nimetöntä. (Your Dictionary.)

Anonymiteetti käsitteenä on ihmisille varmasti tuttu, mutta sen määritelmä voi olla hyvin häilyvä asiayhteydestä riippuen. Pääsääntöisesti anonyymiudella tarkoitetaan nimettömänä pysymistä siten, ettei muilla osapuolilla ole mahdollista saada selville henkilön nimeä tai henkilöllisyyttä. Tästä konkreettisena esimerkkinä ovat internetin anonyymit keskuste-

lupalstat, joissa käyttäjät pystyvät olemaan vuorovaikutuksessa keskenään ilman, että joutuvat tunnistautumaan millään tavoin.

2.2 Pseudonyymi ja sen eri muodot

Anonyymiudesta puhuttaessa tulee myös mainita pseudonyymius, joka käytännössä tarkoittaa salanimen tai taitelijanimen taakse piiloutumista. Pseudonyymin käyttö on yleistä sellaisten artistien, kirjailijoiden ja näyttelijöiden keskuudessa, jotka syystä tai toisesta haluavat esiintyä julkisuudessa muulla kuin omalla nimellään. Esimerkiksi kirjailijat turvautuvat usein pseudonyymin käyttöön silloin, kun ovat julkaisemassa uutta teosta, eivätkä halua vanhan tuotantonsa vaikuttavan sen vastaanottoon millään tavoin. (Wisegeek 2014.)

Viihdeteollisuuden parissa työskentelevillä ihmisillä on ollut tapana ottaa taitelijanimiä, joiden turvin he ovat luoneet itselleen julkisuuskuvan, mikä ei välttämättä olisi ollut mahdollista näiden oikeilla syntymänimillä. Nimi Norma Jeane Baker ei välttämättä sano suurimmalle osalle juuri mitään, mutta tämän taitelijanimi Marilyn Monroe sen sijaan on monelle tuttu. (Wisegeek 2014.)

Joissain tapauksissa taiteilijanimen ottaminen on miltei edellytys henkilön menestymisille johtuen heidän etnisistä taustoistaan. Hyvä esimerkki on Estevez-näyttelijäsuku, jonka tunnetuimmat jäsenet Martin ja Charlie käyttävät taiteilijaniminään Sheen sukunimeä, joka on jossain määrin antanut heille etulyöntiaseman verrattuna muihin suvun jäseniin, jotka esiintyvät syntymänimillään. (Wisegeek 2014.)

Toisinaan taiteilijat käyttävät pseudonyymiä pysyäkseen sukupuolineutraaleina tarkoittaen sitä, että heidän julkisuudessa käyttämästään nimestä on mahdotonta sanoa onko kyseessä mies vai nainen. Tästä oiva esimerkki on Harry Potterin luoja Joanne Kathleen Rowling, joka ennen maailmaan kuuluisuuttaan oli sitä mieltä, että hänen kirjoillaan olisi parempi mahdollisuus menestyä, mikäli lukijat eivät tietäisi hänen olevan nainen ja päätyi käyttämään kirjailijanimessään ainoastaan nimikirjaimiaan. (Wisegeek 2014.)

Tänä päivänä pseudonyymin käyttö on yleisintä Internetin keskustelufoorumeilla, joilla käyttäjät harvoin esiintyvät omilla nimillään. Yleinen käytäntö useimmilla verkkosivuilla onkin, että käyttäjät luovat itselleen nimimerkin, jolloin he voivat vapaammin jakaa mielipiteitään ja käydä keskustelua muiden käyttäjien kanssa. Nimimerkin takaa kommentointi saattaa johtaa erinäisiin ongelmiin käyttäjien kesken, joita käsitellään tekstissä myöhemmin.

3 Verkkoanonymiteettiin liittyvä lainsäädäntö

Yleisesti ottaen Internetin lainsäädäntö on hyvin laaja ja monimutkainen kokonaisuus. Tällä hetkellä näyttääkin siltä, ettei esimerkiksi tekijänoikeuslain kaltaisia globaaleja säädäntöjä tulla näkemään Internetin suhteen aivan lähitulevaisuudessa. Tämä johtuu ensinnäkin siitä, ettei Internet ole minkään tietyn tahon omistuksessa, eikä kenelläkään näin ollen ole minkäänlaista laillista oikeutta tehdä siihen koskevia globaaleja päätöksiä.

Tämän lisäksi Internetin käyttäjäkunta koostuu karkeasti arvioiden reilusta 3 miljardista käyttäjästä, jotka puolestaan edustavat noin kahtasataa eri kansalaisuutta. Näistä jokaisella kahdella sadalla valtiolla on oma kansallinen lainsäädäntönsä, joka eittämättä olisi hidaste, ellei jopa este yhteisten lakien syntymiselle. (Internet Live Stats 2014.)

Vaikka Euroopan unioni ja erinäiset kaupalliset sopimukset ovat osoittaneet, että yhteisten lakien ja säädöksien noudattaminen eri valtioiden kesken on jossain tapauksissa toimiva vaihtoehto, niin saman periaatteen soveltaminen valtavan tietoverkon hallinnointiin ja valvomiseen ei tällä erää vaikuta toimivalta ratkaisulta.

3.1 Yksityisyys perusoikeutena

Yksityisyys on perusoikeus siinä missä sananvapaus tai yhdenvertaisuuskin, joiden varjelemista on pyritty turvaamaan erinäisillä lakipykälillä, niin Suomen kuin Euroopan unionin taholta. Sosiaalisen median käytön lisääntyminen viime vuosina on vaikuttanut merkittävästi myös ihmisten suhtautumiseen yksityisyyttään kohtaan. Euroopan unionin vuonna 2011 teettämästä europarametrista käy ilmi, että lähes 75 % unionin kansalaisista on sitä mieltä, että henkilökohtaisten tietojen luovuttaminen tai jakaminen on osa kehittyvää nykyyhteiskuntaa. Pääsääntöisesti käyttäjät luovuttavat tietojaan erinäisten internetin verkkopalveluiden ja sovellusten käyttöön. Vastineeksi he saavat oikeuden käyttää kyseisiä palveluita. (Euroopan unioni 2011, 6.)

Samaisesta tutkimuksesta käy ilmi, että vaikka ihmiset vapaaehtoisesti luovuttavat tietojaan, eivät he kuitenkaan ole luottavaisia sen suhteen, etteikö kyseisiä tietoja voitaisi käyttää johonkin muuhunkin tarkoitukseen kuin mihin ne alun perin oli tarkoitettu. Vajaa puolet kyselyyn vastanneista oli sitä mieltä, että EU-tasolla tulisi päättää keinoista ja asetuksista, joilla pyrittäisiin ehkäisemään henkilötietojen laitonta käyttöä. Tällaisia menetelmiä olisivat muun muassa sakkorangaistukset, henkilötietojen käyttökiellot sekä korvaukset niille asianomaisille, joiden tietoja tahot ovat luvatta käyttäneet. (Euroopan unioni 2011, 8.)

Yksityisyys on ja on ollut itsestäänselvyys näihin päiviin saakka. Tilanne kuitenkin saattaa muuttua lähitulevaisuudessa, mikäli on uskominen tietovuotaja Edward Snowdeniin. Hän totesi brittiläisen Channel 4:n haastattelussa, että tulevat sukupolvet saattavat kasvaa yhteiskunnassa, jossa ei ole minkäänlaista käsitystä yksityisyydestä. Tällä hän viittaa tosiasiaan, että jo tänä päivänä kannamme mukanamme laitteita, jotka seuraavat liikkeitämme missä ikinä liikummekaan ja voidaan vain olettaa, että tilanne tulee ainoastaan kärjistymään seuraavien vuosikymmenten aikana. (Channel 4 2013.)

3.2 Yksityisyyden suoja Suomen lainsäädännössä

Suomen lainsäädännöstä yksityisyyttä ja sen turvaamista säänteleviä lakeja ovat Henkilötietolaki 22.4.1999/523, Laki yksityisyyden suojasta työelämässä 13.8.2004/759 sekä Sähköisen viestinnän tietosuojalaki 16.6.2004/516. Kaikkien edellä mainittujen lakien tarkoituksena on taata Suomen perustuslain mukainen oikeus yksityisyyden suojaan. Näiden lisäksi meitä suojelevat myös Euroopan unionin asettamat direktiivi Henkilötietodirektiivi (46/1995/EY) ja Sähköisen viestinnän tietosuojadirektiivi (58/2002/EY). (Yksityisyydensuoja 2014b.)

Henkilötietolaki

Ensimmäisenä mainitun henkilötietolain perusperiaatteena on ajaa yksityiselämän suojaa ja samalla edistää hyvän tietojenkäsittelyntavan kehittämistä ja noudattamista. Lain alaisuuteen katsotaan kuuluvan kaikki toiminta, missä henkilötietoja käsitellään automatisoidusti. Tarvittaessa lakia voidaan myös soveltaa tilanteisiin, joissa henkilötietojen katsotaan muodostavan henkilörekisterin tai jonkin sen osan. Henkilötietolain katsotaan olevan käypä silloin, kun rekisteriä pitävän tahon toimipaikka on Suomessa tai tilanteissa, jossa rekisterinpitäjä toimii EU:n ulkopuolisesta valtiosta käsin, mutta käyttää Suomessa sijaitsevia laitteistoja datan prosessointiin tai mihin tahansa muuhun toimenpiteeseen kuin tietojen siirtoon. (Henkilötietolaki 22.4.1999/523.)

Laki yksityisyyden suojasta työelämässä

Lain yksityisyyden suojasta työelämässä tarkoituksena on ajaa suomalaisten yksityisyyden suojaa turvaavia perusoikeuksia työelämässä. Laissa määritellään muun muassa millä tavoin työnantajan tulee käsitellä työntekijöidensä henkilötietoja, miten työntekijöitä saa testata tai tarkastaa, millainen työntekijöihin kohdistuva tekninen valvonta työpaikalla on sallittua sekä paljon viime vuosina julkisuudessa puhuttanut sähköpostiviestien käsittely ja lukeminen. (Laki yksityisyyden suojasta työelämässä 13.8.2004/759.)

Sähköisen viestinnän tietosuojalaki

Sähköisen viestinnän tietosuojalaki puolestaan on merkittävin laillinen suoja, jonka Suomen lainsäädäntö tarjoaa verkon käyttäjille. Sen tarkoituksena on turvata sähköisen viestinnän luottamuksellisuus, varmistaa yksityisyyden suojan toteutuminen ja samalla edistää sähköisen viestinnän tietoturvaa sekä kehittää sähköisen viestinnän palveluiden kehittymistä. (Sähköisen viestinnän tietosuojalaki 16.6.2004/516.)

3.3 Electronic Frontier Finland ja muut sähköisiä oikeuksia puolustavat järjestöt

Maa- ja unionikohtaisten lainsäädäntöjen lisäksi ihmisten turvana on järjestöjä, joiden tarkoituksena on puolustaa kansalaisten yksityisyyttä sekä muita sähköisiä oikeuksia. Merkittävin Suomessa toimiva taho on voittoa tavoittelematon *Electronic Frontier Finland ry* (EFFI), jonka toiminta alkoi vuonna 2001 siitä syystä, että Suomesta puuttui organisaatio, joka puuttuisi yksittäisten Internetin käyttäjien ja ohjelmoijien yksityisyyttä ja sananvapautta uhkaaviin epäkohtiin. EFFI:n perustajajäsenillä oli alusta asti tarkoituksena ottaa mallia Yhdysvalloissa toimivasta *Electronic Frontier Foundationista (EFF)* soveltamalla sen ideologiaa ja toimintamalleja Suomen normeihin sopiviksi. (Välimäki 2004, 2.)

EFFI:n panostus informatiivisena tiedonjakajana ja kansalaisten perusoikeuksien suojelijana reilun 10 vuoden aikana on ollut hyvin merkittävä. Ensimetreillään EFFI:llä oli pienimuotoisia ongelmia tulla kuulluksi, joka johtui pääosin siitä, etteivät valtamediat juurikaan noteeranneet sen lausuntoja. Kaikki kuitenkin muuttui syyskuussa 2002 Myyrmannin pommi-iskun myötä, jonka johdosta mediassa käsiteltiin asian tiimoilta myös nettisensuurin tarpeellisuutta ja EFFI:n tutkijoita kutsuttiin useampiin tv-haastatteluihin keskustelemaan asiasta. (Välimäki 2004, 7-8.)

EFFI:n toiminta ei ole rajoittunut yksinomaan Suomen rajojen sisälle vaan järjestö oli mukana vuonna 2002 perustamassa European Digital Rightsia (EDRi), joka on Euroopan vastine EFFI:lle ja EFF:lle. Ennen EDRi:n perustamista EFFI:n jäsenet olivat kaavailleet itse perustavansa EFF Europen, mutta ajankäyttöön liittyvistä ongelmista johtuen EFFI hylkäsi kunnianhimoisen hankkeensa, jonka jälkimainingeista EDRi muovautui. (Välimäki 2004, 12.)

Edellä mainittujen järjestöjen lisäksi eri puolilla maailmaa on vastaavanlaisia tahoja, joiden tarkoituksena on suojella ihmisten yksityisyyttä. Tähän kategoriaan kuuluu muun muassa vuonna 2011 Yhdysvalloissa perustettu Fight for the Future, joka on EFFI:n tapaan voittoa tavoittelematon järjestö. Sen perusperiaatteena on edistää sananvapauden ja yksityisyy-

den toteutumista sekä saada näkyvyyttä tekijänoikeuksia käsitteleviin lakeihin. (Fight for the Future 2014.)

3.4 Yhteenveto

Tällä hetkellä on mahdotonta sanoa millä tavoin anonymiteettiä ja yksityisyyttä koskevat lait tulevat muuttumaan lähitulevaisuudessa. Suurimpana kysymysmerkkinä on, löytävätkö päättävät tahot yhteisiä kansainväliä pelisääntöjä joiden avulla pystyttäisiin järkevästi turvaamaan verkonkäyttäjien oikeudet eri puolilla maailmaa.

Suomen ja Euroopan unionin lainsäädännön alaisuudessa olevien käyttäjien tilanne on maailmanlaajuisesti tarkasteltuna loistava. Tällä hetkellä yksityisyyttä koskeva lainsäädäntö pyrkii ainoastaan parantamaan käyttäjien identiteettien turvaa, ennaltaehkäisemään henkilötietoihin kohdistuvat väärinkäytökset sekä edistämään yksityisyyden suojan toteutumista.

Toistaiseksi Suomen lainsäädäntöön ei näytä olevan tulossa suuria muutoksia, joilla pyrittäisiin rajoittamaan yksilöiden sananvapautta tai muutoinkaan estämään verkossa tapahtuvaa toimintaa. Toisaalta parin vuoden takaa löytyy ennakkotapaus, jolloin Sonera ja muut Internet-palveluntarjoajat määrättiin oikeuden toimesta estämään pääsyy The Pirate Bay nimiselle torrent seurantapalvelimelle. Kyseinen esto astui voimaan, koska kyseisen sivuston katsottiin loukkaavaan tekijänoikeuslakia (Sonera). Tämän kaltainen internetsensuuri on Suomessa hyvin poikkeuksellista ja erittäin todennäköisesti vastaavanlaisia toimenpiteitä ei lähitulevaisuudessa tulla näkemään.

Kaiken kaikkiaan yksityisyyden suoja ja sitä säätelevät lait ovat suomalaisten käyttäjien kannalta hyvässä asemassa. Tällä hetkellä ainoana varteenotettavana ongelmana voidaan pitää Yhdysvaltoja, missä valtaosa käyttämistämme verkkopalveluista fyysisesti sijaitsee. USA:n kongressissa käsitellään tuon tuosta uusia lakialoitteita, jotka toteutuessaan mahdollistaisivat entistä laajamittaisemman käyttäjiin kohdistuvan valvonnan ja pahimmassa tapauksessa niitä saatettaisiin tulevaisuudessa soveltaa myös Yhdysvaltojen ulkopuolella toimiviin käyttäjiin.

4 Verkkoanonymiteetti

Luvussa 2. käsiteltiin anonymiteetin yleistä määritelmää ja sen eri muotoja. Tässä luvussa paneudutaan verkkoanonymiteettiin: mitä se on, miten kotikäyttäjät siitä hyötyvät ja minkälaisia sivuvaikutuksia se aiheuttaa. Verkkoanonymiteetin määritelmä on hyvin samantapainen kuin niin sanotun normaalin anonymiteetinkin ja sen katsotaan toteutuvan silloin, kun käyttäjä pystyy pitäytymään tunnistamattomana tilanteissa, jotka tapahtuvat verkossa asioidessa. Tällaisia toimintoja ovat esimerkiksi luvussa kaksi mainittu viestiminen muiden käyttäjien kanssa keskustelufoorumien ja pikaviestiohjelmien välityksellä, sähköpostien lähettäminen, verkkopelaaminen, ostosten tekeminen verkossa tai aivan normaali surffailu verkkosivustoilla. (Nissenbaum 2014.)

4.1 Verkkoanonymiteetin hyödyt

Miten käyttäjät sitten hyötyvät anonyymiydestään verkossa asioidessaan? Ensinnäkin se tukee perusoikeuksiemme toteutumista, kuten Suomen perustuslaissa on määritelty. Anonymiteetti antaa yksilöille mahdollisuuden kommunikoida vapaasti verkon välityksellä muiden käyttäjien kesken ja hakea näiltä apua vaikeidenkin asioiden käsittelyyn, joista puhuminen julkisesti voi olla hankalaa ja jopa noloa. Tällaisesta menettelystä voi olla erityisen suuri apu vakavasta sairaudesta kärsiville tai henkilöille, jotka ovat esimerkiksi toipumassa raskaasta erosta ja hakevat apua kohtalotovereiltaan.

Tämän lisäksi Internet on täynnä sivustoja, joilla ihmiset voivat häpeilemättä avautua tunnontuskistaan ilman pelkoa siitä, miten heidän lähipiirinsä mahtaisi reagoida, mikäli saisivat tietää asiasta. Verkossa avautumista voidaankin jossain määrin verrata ripittäytymiseen papille, joskin ripittäjän roolissa toimivat muut Internetin käyttäjät. Huomioitavaa kuitenkin on, että kannattaa aina lähtökohtaisesti suhtautua hieman kriittisesti Internetissä tapahtuvaan kirjoitteluun varsinkin, jos kyseessä on anonyymi käyttäjä. Anonymiteetin turvin ihmiset voivat myös ottaa kantaa arkaluontoisiin aiheisiin tuoden esille omia rehellisiä mielipiteitään, joka ei välttämättä toteutuisi, mikäli keskustelupaikkana olisi internetin keskustelufoorumin sijaan vaikkapa työpaikan kahvihuone.

Nykypäivänä Internetin tarjoama mahdollisuus reaaliaikaiseen tiedon levitykseen on mahdollistanut uutisoinnin myös maissa, joissa kansalaisten tekemisiä valvotaan järjestelmällisesti ja uutisvirtaa kontrolloidaan - kuten parhaaksi nähdään. Verkkoanonymiteetin ansioista näissä poliisivaltioissa ja totalitaristisissa maissa asuvat ihmiset pystyvät jakamaan informaatiota maansa tilanteesta sosiaalisen median kautta. Loistava esimerkki tästä on helmikuussa 2014 alkaneet levottomuudet Venezuelassa, joista ei tuohon aikaan uutisoitu

juuri lainkaan valtamedioissa vaan kaikki saatavilla oleva informaatio tuli valtaosin sosiaalisen median välityksellä. (One Young World 2014.)

4.2 Verkkoanonyymiuden ongelmat ja epäkohdat

Vaikka anonymiteetti verkossa antaa käyttäjille edellä mainittujen kaltaisia vapauksia, niin sen piiriin kuuluu myös tietynlaisia ongelmia ja epäkohtia, jotka ovat tuttuja Internetin ulkopuolelta. Näitä ovat muun muassa kiusaaminen, uhkailu sekä turhanpäiväisten huhujen levittäminen, jotka ovat arkipäivää erinäisillä verkkosivustoilla. Kyseiset ilmiöt rehottavat, koska nimimerkkien taakse piiloutumista tai nimettömästi tapahtuvaa toimintaa on vaikeaa jäljittää eikä kiinni jäämisen pelkoa juuri ole.

4.2.1 Trollit ja trollaaminen

Ehkä yleisin verkkoanonyymiuden lieveilmiöistä on erinäinen häiriköinti, joka internetissä tunnetaan yleisesti ottaen *trollaamisena*. Tämän kategorian alaisuuteen voidaan käytännössä lukea lähestulkoon kaikki toisiin käyttäjiin kohdistuva pilailu. Tätä provosoivaa käytöstä harjoittavien henkilöiden tai tahojen tarkoituksena on saada toiminnallaan aikaan sekasortoa ja vihastusta muiden käyttäjien keskuudessa. Pääsääntöisesti tätä tapahtuu Internetin keskustelupalstoilla, mutta se ei ole tavatonta muissakaan verkkoympäristöissä kuten verkkopeleissä. Kyseinen termi on kehittynyt internet-yhteisöissä englanninkielen vetouistelu (trolling) sanasta, joka havainnollistaa hyvin trollien (joina nämä Internetin kiusankappaleet tunnetaan) päämäärää saada joku hyväuskoinen käyttäjä tarttumaan heidän syöttiinsä, joka näissä tapauksissa on joko harhaan johtava neuvo tai absurdi lausunto, jolla saadaan aiheutettua keskustelua muiden käyttäjien keskuudessa. Helpoiten tämä on havaittavissa esimerkiksi Youtuben kommenttiosioissa, joissa sananvaihto on yleensä kiivaasta ja yltyy toisinaan hyvinkin asiattomaksi. (Urban Dictionary.)

Loistava esimerkki puolestaan harhaanjohtavasta ja pahansuovasta neuvojen jakamisesta on Applen iPhonen omistajiin kohdistunut toistuva pilailu viime vuosien aikana. Kun Apple julkaisi iOS käyttöjärjestelmän seitsemännen järjestelmäpäivityksen syyskuussa 2013, 4chan foorumin käyttäjät lanseerasivat informatiivisen mainoskampanjan (Liite 1), jonka mukaan kyseinen päivitys tekee puhelemista vesitiiviitä. Tämä sai lukuisat käyttäjät kokeilemaan kyseistä ominaisuutta ja kuten arvata saattaa, eivät puhelimet sietäneet kosteutta alkuunkaan, minkä johdosta Twitter ja muut sosiaalisen median palvelut tulvivat vihaisten ja huijatuksi tulleiden käyttäjien viesteistä. (Gibbs 2013.)

Noin vuosi iOS 7-episodin jälkeen Apple julkisti jälleen uuden järjestelmäpäivityksen iOS 8:n ja tälläkin kertaa 4chan päätti koota rivinsä ja aiheuttaa sekasortoa iPhone-käyttäjien

keskuudessa. Edellisvuoden onnistunut pila suorastaan kannusti ryhmää vastaavanlaiseen tempaukseen ja juntta kehittelikin kerrassaan katalan tempun: langaton lataaminen mikroaaltouunin avulla. Pelkällä maalaisjärjelläkin tämä kuulostaa aivan tolkuttomalta idealta, mutta hyväuskoiset uhrit päätyivät käräyttämään puhelimiensa lisäksi myös mikroaaltouuninsa ja myös tällä kertaa sosiaalinen media täyttyi räyhäävien käyttäjien vihaisista viesteistä. Mikäli sama kaavaa jatkuu niin on odotettavista, että ryhmittymällä on yhtä viheliäisiä ideoita ensi vuodeksi kaavaillun iOS 9:n suhteen. (Tamblyn 2014.)

Vaikka trollaamisen kohteeksi joutuneille käyttäjille tai tahoille saattaa kyseisestä toiminnasta koitua jonkin asteista mielipahaa, on sen lähtökohtaisena tarkoituksena ainoastaan viihdyttää muita yhteisön käyttäjiä. Toki on myös huomioitavaa, etteivät pilailun kohteeksi joutuneet käyttäjät välttämättä ole kauhean otettuja saamastaan huomiosta ja joskus hyväntahtoinenkin trollaus saattaa kääntyä päälaelleen ja seuraukset voivat olla kohtalokkaat. Trollaamista ei tule kuitenkaan sekoittaa sellaisiin käyttäjiin, joiden perimmäisenä tarkoituksena on ainoastaan vahingoittaa muita käyttäjiä henkisellä väkivallalla lähettämällä näille ilkeitä tai rasistisia viestejä. Tällaiset käyttäjät eivät ole trolleja vaan internetkiusaajia joiden toiminta on vastenmielistä ja tuomittavaa.

Turhan usein, kun silmiin osuu otsikko jonkin verkkolehden sivuilla, joka näyttäisi alustavasti käsittelevän trollaamista, niin tarkempi lueskelu paljastaa sen olevankin uutinen internetkiusaamisesta. Toki näissä molemmissa käsitteissä on samoja piirteitä, mutta merkittävä erottava tekijä näiden kahden välillä on niitä harjoittavien käyttäjien päämäärissä. Siinä missä trolli pyrkii ainoastaan saamaan vastapuolen reagoimaan tämän viesteihin tai toimintaan, niin kiusaaja pyrkii henkisesti vahingoittamaan uhriaan. Eroavaisuuksia on myös toimintojen kestossa ja lopputuloksessa. Trollaaminen on yleisesti ottaen hyvin lyhyt toimitus, joka yleisesti ottaen kuihtuu jo kasaan ennen kuin on ehtinyt edes alkaa, koska muut käyttäjät tiedostavat trollien olemassa olon eivätkä tartu niin sanottuihin syötteihin kovinkaan helposti. Toisinaan taitava ja viekas käyttäjä onnistuu trollaamaan toista hyväuskoista käyttäjää tai tahoa, jonka seurauksena yhteisössä naureskellaan asialle hetken tai kaksi, minkä jälkeen asiaa ei sen koomin muistella. Internetkiusaamisella sen sijaan on pysyvämmät vaikutukset ja sen kesto saattaa tilanteesta riippuen kestää jopa vuosia, minkä johdosta myös siitä koituvat seuraamukset ovat huomattavan paljon vakavammat.

Viime aikoina huolestuttavan paljon lisääntynyt ilmiö on swattingiksi kutsuttu trollaamisen muoto, joka on aiheuttanut päänvaivaa etenkin Yhdysvalloissa. Swatting ei sinänsä ole mikään aivan uusi ilmiö, mutta se on saanut tuulta alleen viime vuosina erityisesti Internetin peliyhteisöissä, kun swattingin kohteeksi on joutunut henkilöitä, jotka lähettävät reaali-

aikaista videokuvaa pelisessioistaan ja koko poliisioperaatio on ollut koko kansan nähtävillä. (Goldstein, S 2014.)

Swattingia harjoittava henkilö soittaa perättömän hätäpuhelun poliisille väittäen, että käynnissä on tilanne, joka vaatii viranomaisten pikaista väliintuloa. Soittaja voi esimerkiksi väittää pitävänsä panttivankeja tai, että hänellä on hallussaan pommi, jonka on aikeissa räjäyttää. Nykyteknologian avuin soittajalla on mahdollisuus peittää oman puhelinnumeronsa ja samalla luoda vaikutelma, että puhelu tuleekin swattingin kohteeksi joutuvalta henkilöltä, minkä seurauksena raskaasti aseistautuneet poliisit rynnäköivät viattoman henkilön kotiin. (FBI 2008.)

4.2.2 Nuoret ja internet-kiusaaminen

Internet-kiusaaminen on yleisintä nuorten keskuudessa ja on jossain määrin verrattavissa koulukiusaamiseen. Useimmissa tapauksissa kiusaaja ja kiusattu tuntevat toisensa, mutta yleistä on myös, ettei uhrilla ole mitään tietoa kiusaajansa henkilöllisyydestä. Tällainen toiminta tapahtuu pääsääntöisesti internetin keskustelufoorumeilla kuten Suomi24:ssä tai muissa vastaavissa virtuaaliympäristöissä, joissa nuoret ovat vuorovaikutuksessa keskenään, kuten esimerkiksi verkkopohjaisissa tietokone- tai konsolipeleissä. Nettikiusaaminen on yhtä tuomittavaa siinä missä perinteinenkin kiusaaminen, mutta valitettavan usein nettikiusaamisen uhrit jäävät ilman huomiota, koska siihen puuttuminen on huomattavan paljon vaikeampaa. (Sourander 2010.)

Valitettavan usein mediassa uutisoidaan tapauksista, jotka ovat äityneet niin pahoiksi, että nuori henkilö on päättänyt riistää itseltään hengen internet-kiusaamisen seurauksena. Tällaiset henkilöt ovat mitä todennäköisimmin kärsineet koulu- ja internet-kiusaamisesta jo useamman vuoden ajan ja jossain välissä tulee vastaan tilanne, jossa henkilö on päättänyt luovuttaa. Koulussa tapahtuvaan kiusaamiseen pystytään puuttumaan opettajien ja vanhempien toimesta, mutta verkossa tapahtuva kiusaaminen jää yleensä huomaamatta ja tilanteen vakavuus paljastuu vasta, kun on jo liian myöhäistä.

Siinä missä kiusaaminen aikaisemmin rajoittui tiettyyn paikkaan, kuten esimerkiksi kouluihin, niin nykyään kiusaajat pystyvät piinaamaan uhrejaan myös verkon välityksellä, eivätkä nämä välttämättä ole turvassa edessä kotonaan. Koulukiusaamisesta voi päästä eroon vaihtamalla koulua ja asuinaluetta, mutta verkossa nuoren piinaaminen voi jatkua ympäristön vaihdoksesta huolimatta. Merkittävä ongelma erityisesti nuorten keskuudessa on perättömien huhujen tai arkaluonteisen materiaalin levittäminen, kuten Amanda Toddin tapaus osoittaa (Kuva 1). Verkkoon päätynyt kuva sysäsi nuoren tytön syöksykierteeseen,

johon ei auttanut edes koulun tai kaupungin vaihdos. Tyttö masentui, muuttui apaattiseksi ja itsetuhoiseksi ja vei itseltään lopulta hengen. (No Bullying 2014). Amandan tapaus keräsi paljon huomiota ja herätti keskustelua internet-kiusaamisen tiimoilta. On kuitenkin valitettavaa, että jotain näin traagista täytyy tapahtua ennen kuin ihmiset alkavat reagoimaan.

Kuva 1. Amanda Todd avautui karusta kohtelustaan Youtubessa (No Bullying 2014)

Lasten Internetin käytön rajoittamisesta ja valvomisesta on käyty keskusteluja koko 2000-luvun ajan. Vanhempien rooli on totta kai merkittävä ja heidän vastuullaan on pitää silmällä jälkikasvunsa internetin käyttöä ja pyrkiä vaikuttamaan, ettei omasta lapsesta vartu muita nuoria terrorisoiva häirikkö. Myös koulujen tulisi panostaa enemmän verkossa tapahtuvan kiusaamisen ehkäisemiseksi. Toisaalta kiusaajia ja kiusattuja on aina ollut, mutta ehkä riittävän aikaisessa vaiheessa nuorten toimintaan puuttumalla pystyttäisiin estämään Amanda Toddin kaltaisten skenaarioiden syntyminen.

Sosiaalinen media antaa käyttäjilleen paljon vapauksia, mutta myös vastuuta. Nuori voi pitää hauskana pilana koulukaverinsa alastonkuvan levittämistä esimerkiksi Facebookissa, mutta tästä voi aiheutua vakavia sanktioita, joita nuori ei välttämättä tiedosta. Pahimmassa tapauksessa tämä voidaan rekisteröidä seksuaalirikolliseksi ja nuoresta iästään johtuen myös tämän vanhemmille saattaa koitua seuraamuksia nuoren toilailuista. (Bullying Statistics 2013.)

4.2.3 Rikollisuus

Vakavimmat verkkoanonymiteetin lieveilmiöistä ovat organisoituneen rikollisuuden harjoittamat huume- ja ihmiskauppa sekä lapsipornoringit, jotka toimivat Internetin ”syövereissä”,

- poissa tavallisen kotikäyttäjien näkyviltä. Tätä Internetin osaa kutsutaan deep webiksi siitä syystä, että normaalit hakukoneet eivät löydä tai pääse käsiksi näihin sivustoihin ja niistä löytyvään dataan.

Tavallisimmilla verkonkäyttäjillä tuskin on aavistustakaan siitä palveluiden kirjosta, joka internetistä on saatavilla. Vuosien varrella käyttäjillä on ollut mahdollisuus tilata vaivatta esimerkiksi huumeita suoraan kotiovelleen erinäisten verkkosivustojen kautta, kuten Daily Mirrorin tekemästä reportaasista käy ilmi. (Myall, S. 2014.) Myallin mainitsema sivusto on sittemmin jo suljettu viranomaisten toimesta, mutta voi vain arvailla kuinka paljon vastaavanlaisia sivustoja ja palveluita on edelleen toiminnassa. Tilanteeseen tuskin on luvassa sen suurempia muutoksia lähiaikoina, elleivät viranomaiset löydä uusia ja tehokkaampia menetelmiä tämän kaltaisen liiketoiminnan kitkemiseksi, koska aivan varmasti jotkin tahot pyrkivät hyödyntämään näitä menetelmiä prikulleen niin kauan kuin kyseinen liiketoiminta pysyy tuottoisana.

Huumekaupan lisäksi deep webin syövereistä on mahdollista löytää erinäinen määrä hämärän puoleisia sivustoja ja keskustelupalstoja, joiden kautta voidaan muun muassa ostaa vaikkapa varastettuja henkilötietoja, laittomia aseita ja palkata jopa palkkamurhaajia (Jaeger 2012). Eettisistä syistä en lähde sen tarkemmin tutustumaan ja kartoittamaan, mistä tällaisia sivustoja on mahdollista löytää, koska pelkästään jo tieto niiden olemassa olosta on häkellyttävää.

4.3 Yhteenveto

Kaikista epäkohdista huolimatta verkkoanonymiteetti on rikastuttanut Internetkulttuuriamme niin paljon, että on vaikeaa edes kuvitella, että ihmiset joutuisivatkin esiintymään verkossa omalla nimellään.

Periaatteessa kaikki käyttäjät hyötyvät verkkoanonymiteetin tarjoamista eduista, mutta käytännössä vain murto-osa hyödyntää sen koko potentiaalin. Lähtökohtaisesti käyttäjillä olisi mahdollisuus pysyä nimettöminä verkossa surffaillessaan, mutta nykypäivänä monet käyttäjät ovat lähestulkoon poikkeuksetta kirjautuneina johonkin sosiaalisen median palveluun ja näin ollen käyttäjien henkilöllisyys ja niin sanottu verkkominä saattavat linkittyä keskenään, jolloin anonymiteetin säilyminen ei ole enää taattua. Toisaalta on olemassa myös käyttäjiä, jotka todella arvostavat omaa yksityisyyttään ja pitävät sen paljastumista suurena uhkana, minkä johdosta omaa anonymiteettiä pyritään varjelemaan kaikin mahdollisin keinoin. Tällöin ei riitä pelkästään nimettömänä pysyminen, vaan kaikki toiminta

verkossa pyritään peitellä esimerkiksi naamioimalla oma IP-osoite näyttämään joltain aivan muulta, mikä se todellisuudessa olisi.

On säälittävää nähdä yksittäisten käyttäjien tahraavan verkkoanonymiteetin tarjoamat mahdollisuudet typerällä käytöksellään, koska mediassa uutisoidaan ainoastaan anonymiteetin aiheuttamista haitoista ja asiaan perehtymättömät saattavatkin saada sellaisen käsityksen, että sillä on ainoastaan negatiivinen vaikutus käyttäjiin.

Yleisesti ottaen verkkoanonymiteetin hyödyt ja haitat on helposti listattavissa, mutta kun niiden vaikutuksia ruvetaan tarkastelemaan yksilötasolla, ei asia olekaan niin yksinkertainen. Toiset käyttäjät voivat päätyä internet-kiusaamisen kohteeksi toisia helpommin tai tarttuvat trollien viesteihin muita hanakammin ja näin ollen altistavat itsensä ehdoin tahdoin anonymiteetistä aiheutuville haitoille. Anonymiteetin suurimmat ongelmat muodostuvatkin muiden käyttäjien epäasiallisesta käytöksestä, eikä verkossa tapahtuva rikollinen toiminta juurikaan kosketa tavallisimpia verkonkäyttäjiä.

Tulevaisuudennäkymiä on hyvin vaikea lähteä ennustamaan, mutta mitä todennäköisimmin anonymiteetin aiheuttamat ongelmat eivät ole katoamassa mihinkään, vaan osa käyttäjistä joutuu jatkossakin kärsimään muiden käyttäjien ajattelemattomuudesta. Ongelman laajuutta voitaisiin kuitenkin pyrkiä hillitsemään esimerkiksi valistamalla nuoria internet-kiusaamisesta ja sen aiheuttamista haitoista, mutta käytännössä tämä vaatisi toteutuakseen suunnattomia ponnisteluja niin kansallisella kuin kansainvälisellä tasollakin. Näin ollen voidaan olettaa, että tilanne tulee etenemään vain omalla painollaan ja vasta vuosien saatossa tullaan näkemään muuttuuko ihmisten verkkokäyttäytyminen suuntaan tai toiseen.

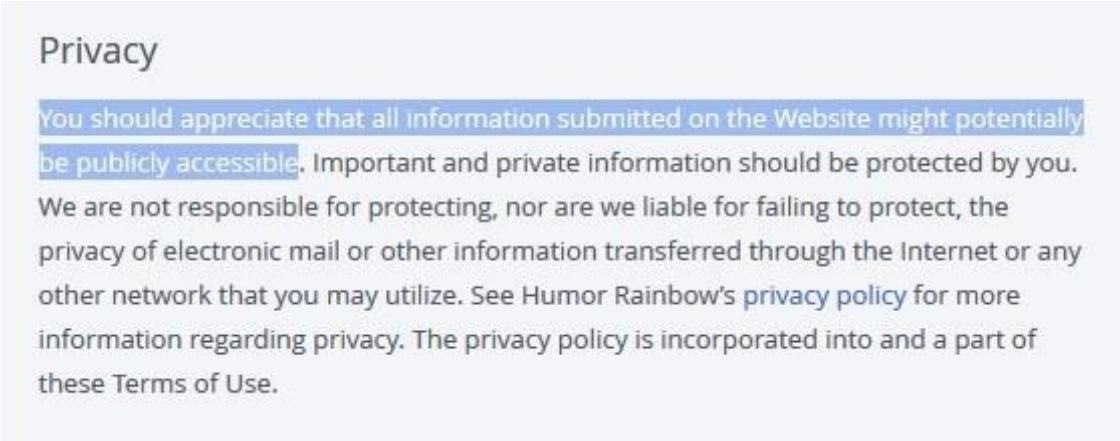
5 Tiedonkeruu ja verkkomainonta

Markkinointiyritysten ja tiettyjen suurten organisaatioiden harjoittama tietojenkeruu ei sinällään ole mikään uusi juttu: Yritykset ovat harjoittaneet asiakaskuntansa ja uusien potentiaalisten asiakkaiden kartoittamista jo vuosikymmenten ajan analysoimalla esimerkiksi heidän luottokorttiostoksiaan, jonka avulla on saatu selville ihmisten kulutustottumuksia. Vasta aivan viimeisten vuosien aikana tietojenkeruuseen käytettyjen resurssien määrä on kasvanut räjähdysmäisesti ja sen ympärille on muodostunut menestyvä liiketoiminnanala. (Kroft 2014.)

Verkossa asioiminen on nykypäivänä niin arkinen askare, ettemme välttämättä kiinnitä huomiota kaikkeen siihen informaatioon, jota luovutamme erinäisten verkkopalveluiden käyttöön. Olipa kyse sitten vain tavanomaisesta verkkosurffailusta tai uuden kodinkoneen tilaamisesta verkkokaupasta, jää transaktiosta sivuston ylläpitäjän haltuun valtavasti tietoa käyttäjästä. Esimerkiksi verkko-ostoksia tehdessämme annamme myyjälle nimitietojemme lisäksi mitä todennäköisimmin myös kotiosoitteemme, puhelinnumeromme, sähköpostiosoitteemme ja joissain tapauksissa myös ikämme. (Federal Trade Commission 2014, 19.) Tämän lisäksi käytössämme on erinäisiä kanta-asiakaskortteja, jotka kirjaavat ostostottumuksistamme, jotta yritykset osaavat kohdistaa mainoksiaan ja alennuksiaan tietyille asiakkaille (Marketing-Schools 2012). Suomessa tällaista toimintaa harjoittaa esimerkiksi Kesko, jonka K-Plussa-kortteja on yhtymän verkkosivujen mukaan liki 4 miljoonalla suomalaisella (Plussa 2014).

Verkkokäyttäytymisellämme pystymme vaikuttamaan siihen, kuinka paljon informaatiota meistä on saatavilla Internetissä. Tuskin kovinkaan moni tulee edes ajatelleeksi sitä, kuinka paljon ylimääräistä tietoa heistä on saatavilla perustuen siihen, millä tavoin he ovat tottuneet käyttämään sosiaalista mediaa. Tilapäivityksien, kuvien paikannustietojen ja muiden verkossa suorittamien toimenpiteidemme johdosta meistä päätyy, mitä yksityiskohtaisimpia tietoja erinäisten tahojen haltuun. (Kroft 2014.)

Yleensä yritykset tiedottavat sivuillaan kyllä hyvin tarkasti siitä, miten talteen kerättyjen henkilötietojen käsittelyn kanssa menetellään (Kuva 2). Toisinaan nämä lausunnot joko jäävät ihmisiltä lukematta tai sitten he eivät ymmärrä lainkaan vaikeaselkoisia lakitekstejä, kuten käy ilmi Euroopan unionin laatimasta barometristä (Euroopan unioni 2011, 122).



Kuva 2. Ote OkCupid seuranhakupalvelun käyttöehdoista (OkCupid 2014)

Kotikäyttäjän kannalta hanakimmin identiteettiemme perässä ovat Apsilonin, Acxiomin ja Experianin tapaiset markkinointiyritykset. Näistä yrityksistä käytetään nimitystä tiedonkerääjä, data broker. Ne keräävät ja myyvät systemaattisesti ihmisten henkilökohtaisista tiedoista koostuvia informaatiokokonaisuuksia. (Singer 2012.)

Keväällä 2014 Steve Kroft haastatteli eri alojen asiantuntijoita 60 Minuuttia tv-ohjelmaa varten. Kyseisessä jaksossa paneuduttiin tiedonkeruuseen ja sitä harjoittaviin yrityksiin ja tahoihin. Haastatteluissa ilmeni, että tietojen kerääminen ja välittäminen on valtava bisnes, joka on pyritty pitämään poissa suurten massojen tietoisuudesta. Tämän bisneksen tarkoituksena on koota valtavia tietokantoja, jotka pitävät sisällään informaatiota esimerkiksi ihmisten terveydentilasta, luottotiedoista ja perhe-elämästä. Tätä informaatiota seulomalla voidaan luoda kategorisoituja listoja henkilöistä, joilla kaikilla on jokin yhdistävä tekijä. Tämän jälkeen yrityksillä on kaupallinen hyödyke, jota ne voivat kaupata eteenpäin tahoille, jotka ovat kiinnostuneita tietyn kategorian alaisuuteen listautuvista henkilöistä. Tällaisia tahoja voivat olla vaikkapa pankit, jotka haeskelevat tietyn ikäisiä tai vaurausasteeltaan sopivanlaisia henkilöitä laina- tai rahoitushankkeisiin. Vaihtoehtoisesti informaation kerännyt yritys voi hyödyntää sitä omassa toiminnassaan. (Kroft, 2014.)

5.1 Tietokantamarkkinointi

Tietojenkeruun tuloksena muodostuvat valtavat tietokannat toimivat oleellisena osana verkossa tapahtuvaa mainontaa, josta saadun informaation avulla mainostajat pystyvät tarjoamaan kuluttajille näiden kiinnostuksen kohteina olevia tuotteita tai palveluita. Tätä kyseistä menettelytapaa kutsutaankin osuvasti tietokantamarkkinoinniksi, joka on yksi suoramarkkinoinnin muodoista. Kyseistä metodia käyttäen yritykset pystyvät järjestelmällisesti koordinoimaan mainoskoneistonsa siten, että mainokset kohdistetaan sellaisille

käyttäjäryhmille, joita pidetään jo etukäteen potentiaalisina asiakasehdokkaina. (Marketing-Schools 2012.)

Kotikäyttäjän näkökulmasta tämä on helpoiten havaittavissa sähköpostiin saapuvana ”roskapostina” tai fyysisen postin mukana tulevina mainoskirjeinä, jotka ovat kohdistettu nimellä. Tästä havainnollistava esimerkki on miltei jokavuotinen ajoneuvon katsastaminen. Kun auton katsastusleima lähestyy loppuaan, alkaa postiluukusta putoilla lähes päivittäin eri katsastusasemien mainoksia, jotka kehottavat kääntymään heidän palveluidensa puoleen. Tämän lisäksi myös puhelinmyyjät käyttävät työssään tämänkaltaisia kategorisoituja listoja henkilöistä, joille sitten kaupitellaan kaikkea aikakauslehdistä vitamiineihin.

5.2 Online Behavioral Advertising

Yritykset käyttävät mainonnassaan tietokantamarkkinoinnin lisäksi myös muitakin toimintamalleja. Kenties merkittävin on Interest-Based Advertising (IBA) tai Online Behavioral Advertising (OBA), joilla tarkoitetaan eri verkkosivuilla esiintyviä mainoksia, joiden sisältö määräytyy käytännössä sen mukaan millaisilla sivustoilla vierailet. Jos suunnitelmissa on esimerkiksi ulkomaanmatka ja kartoitettaessa varteenotettavia lomakohteita vieraillaan lukuisilla eri matkatoimistojen sivuilla, on hyvin todennäköistä, että jatkossa verkkosivustoilla näkemiesi mainosten sisältö tulee liittymään matkailuun tai valittuun kohdemaahan (Kuva 3). (Network advertising 2012.)

Kuva 3. Havainnollistava kuva siitä miltä Online Behavioral Advertisingin käytännössä näyttää (Network Advertising 2012)

Tässä markkinointimallissa yritykset eivät ole niinkään kiinnostuneita ihmisten yksityistiedoista, vaan tarkoituksena on pääasiallisesti selvittää näiden kiinnostuksen kohteita, jolloin näitä käyttäjiä pystytään lähestymään oikeanlaisella mainonnalla. Tämä tapahtuu käytännössä evästeiden avulla, joita käsitellään hieman tarkemmin tulevissa luvuissa. Perusideana kuitenkin on, että selaimet tallentavat verkkosivujen pyynnöstä tietoja selailutottumuksistamme, kuten millaisten aihealueiden uutisia tai artikkeleita totutusti luemme. Mikäli vierailemme tämän jälkeen jollain toisella verkkosivulla, joka käyttää samaa mainospalve-

luntarjoajaa, niin evästeiden avulla sivulla esiintyvät mainokset osataan jatkossa kohdentaa käyttäjän selailutottumuksia mukaileviksi (Kuva 4). Käyttäjät voivat kuitenkin halutessaan vaikuttaa näiden kyseisten mainosten näkyvyyteen muokkaamalla selaintensa asetuksia ja asentamalla selaimeen mainosten estoon tarkoitettuja lisäosia, joiden avulla pystytään vaikuttamaan merkittävästi mainosten näkyvyyteen. Näitä laajennuksia ja kuinka niitä asennetaan, tutkaillaan hieman tarkemmin evästeiden tapaan luvussa 7. (Network advertising 2012.)

Kuva 4. Karkea luonnos kuinka evästeet toimivat (Network Advertising 2012)

Ihmiset ovatkin ryhtyneet lisääntyvissä määrin käyttämään mainoksia estäviä selainten lisäosia, mikä on saanut mainostajat varpailleen. Adoben ja PageFairin tekemästä tutkimuksesta ilmenee, että vuoden 2014 toisella vuosineljänneksellä arviolta 144 miljoonaa verkonkäyttäjää estää verkossa esiintyvät mainokset. Luku on siinä mielessä merkittävä, että kasvua edellisvuoteen on tullut lähes 70 % ja voidaan vain olettaa, että suunta on nouseva. (Pagefair 2014, 3.)

Tutkimuksen mukaan käyttäjät turvautuvat mainosten estoon pääasiassa siitä syystä, että verkkosivuilla esiintyvät mainosbannerit ja -videot vaikuttavat huomattavasti verkkosurffailun käyttömukavuuteen. (Pagefair 2014, 10) Tutkimusta lukiessaan rupea mietityttämään, miksei siinä ole lainkaan huomioitu mainosten kautta leviäviä haittaohjelmia, joka on varmasti yksi merkittävimmistä syistä, miksi osa käyttäjistä on alun perin ryhtynyt mainoksia estämään. Onko tämä ollut tietoinen valinta jo tutkimuksen suunnitteluvaiheessa, jolla on haluttu vähätellä mainoksista aiheutuvia tietoturvariskejä vai onko kyseessä inhimillinen erehdys?

5.3 Tietojen kerääminen ei-markkinallisista syistä

Sen lisäksi, että yritykset keräävät käyttäjien tietoja kaupallisista syistä, on viime vuosien mediassa puhuttu paljon siitä, kuinka eri maiden hallitukset, erityisesti Yhdysvallat ja etu-

nenässä sen kansallinen turvallisuusvirasto (NSA), ovat harjoittaneet laajamittaista ja systemaattista valvontaa, joka ei ole rajoittunut ainoastaan sen oman maan kansalaisiin. Kyseinen virasto on ollut toiminnassa jo 1950-luvun alkupuolelta saakka ja alun perin sen tarkoituksena oli toimia ainoastaan kulisseissa, poissa julkisuuden valokeilasta. Virasto on kuitenkin muuttanut toimintaperiaatteitaan ja avustaa yhdysvaltalaisia yrityksiä muun muassa tietoturvaa koskevien kysymysten kanssa. (National Security Agency.)

Ehkä merkittävin muutos NSA:n toiminnan kannalta tapahtui syyskuun 11. päivän terroriiskujen jälkeen, kun Yhdysvaltain silloinen presidentti George W. Bush myönsi turvallisuusvirastolle valtuudet valvoa maan kansalaisten puhelinkeskusteluja ja tietoliikenteen vaihtoa ulkomaille pyrkien ennaltaehkäistä New Yorkin ja Washingtonin kaltaisten iskujen toistuminen tulevaisuudessa (Arena 2005). Vaikka yleisesti on tiedostettu, että NSA:lla on valtuudet tietynasteiseen tietoliikenteen valvontaan eikä sen toiminta ole ollut läheskään yhtä salamyhkäistä kuin joitain vuosikymmeniä sitten, niin silti vuoden 2013 kesäkuussa julkisuuteen vuotaneet tiedot viraston laajamittaisesta valvonnasta hätkähdyttivät ihmisiä ympäri maailmaa. Ehkä merkittävin yksittäinen tapaus tässä hyvin sekavassa vakoiluvyyhdissä on ollut väittämä, jonka mukaan Saksan liittokanslerin Angela Merkelin puhelinta salakuunneltiin NSA:n toimesta (Spiegel 2013). Toisaalta maallikoiden on mahdotonta mennä sanomaan, onko väittämässä ollut alun alkaenkaan mitään perää ja kyseinen episodi saattaa jäädä ikuiseksi mysteeriksi.

5.4 Yhteenveto

Yleisesti ottaen voidaan ajatella, että verkkomainontaan ja tietojenkeruuseen suhtautuminen on pääsääntöisesti negatiivista, koska kukapa haluaa ehdoin tahdoin joutua esimerkiksi puhelinmyyjien tai sähköpostiin tulvivien roskapostien kohteeksi. Toisaalta jos mainonnan kohteeksi joutuminen ei tunnu kovinkaan suuresti haittaavaan, voi kohdalle silloin tällöin osua myös otollisia tarjouksia tai ilmaisnäytteitä.

Käyttäjillä on kuitenkin hyvin vähän mahdollisuuksia suojautua verkkomainontaa vastaan ja tilanne vaikeutuu entisestään jos käyttäjän tiedot päätyvät mainostajien tietokantoihin. Verkkosivuilla esiintyvät mainosbannerit pysytään kuitenkin estämään selaimiin saatavien lisäosien avulla, mikä aiheuttaa odotetusti hyvin eriäviä mielipiteitä mainostajien ja käyttäjien keskuudessa. Verkkomainonnan tarpeellisuudesta sekä sen hyödyistä voidaan myös esittää hyvin eriäviä mielipiteitä. Kotikäyttäjän näkökulmasta mainokset tuntuvat varmasti ärsyttäviltä ja turhanpäiväisiltä. Kun niiden tarpeellisuutta ruvetaan tarkastelemaan mainostajien ja palveluidentarjoajien näkökulmasta, on auttamattakin selvää, ettei käyttäjille olisi tarjolla niin laajaa ilmaisten sovellusten ja palveluiden kirjoa kuin, minkä verkko-

mainonta on mahdollistanut. Ilman mainoksista saatavia tuloja valtaosa käyttämistämme verkkosovelluksista ja palveluista olisi mitä todennäköisimmin maksullisia. Olisivatko kotikäyttäjät sitten valmiita maksamaan niiden palveluiden käytöstä, joita ovat jo vuosia tottuneet käyttämään ilmaiseksi?

Toisinaan tietojenkeruusta voidaan katsoa olevan näennäistä hyötyä myös tavallisille käyttäjille, mikäli sen avulla kerättyjen tietojen perusteella pystytään esimerkiksi ehkäisemään terrori-iskujen tai kouluampumisten toteutuminen. Toisaalta tällaisista tilanteista ei kauhean usein uutisoida, joten on erittäin vaikeaa arvioida, kuinka usein esimerkiksi Suomessa esiintyy välikohtauksia, jotka vaativat Suojelupoliisin puuttumista tilanteeseen.

6 Anonyymit verkot

Millä tavoin kotikäyttäjät sitten pystyvät tehostamaan anonyymiyttään verkossa asioidessaan? Tapoja on monia ja niitä tullaan käymään lävitse yksi kerrallaan tulevissa luvuissa. Ensimmäisenä tutustutaan anonyymeihin verkkoihin, joiden avulla käyttäjät voivat halutessaan pysyä nimettöminä. Tämän lisäksi ne mahdollistavat käyttäjille pääsyn käsiksi informaatioon, joka ei ole saatavilla normaaleja Internetin selaustapoja käyttämällä. Näistä verkoista käytetään yleisesti nimitystä darknet. (Yksityisyydensuoja 2014a.)

Tässä luvussa tullaan käsittelemään Tor ja Freenet nimisiä ohjelmistoja, joiden lisäksi tarjolla olisi myös lukuisia muitakin samantyyppisiä ohjelmistoja, kuten esimerkiksi The Invisible Internet Project (I2p) tai GNUnet. Tor ja Freenet vaikuttavat kuitenkin olevan varteenotettavimmat vaihtoehdot, koska ohjelmistoja kartoittaessa niistä tuntui löytävän kaikista eniten taustamateriaalia. Tämän lisäksi valintaan vaikutti myös se tosiasia, että olin tietoinen niiden olemassa olosta jo enne työn aloittamista, joten myös tästä syystä niiden valinta tuntui ilmeiseltä.

6.1 Tor Project

Epäilemättä tunnetuin tämän kategorian palveluista on sipulireititys eli Tor (The Onion Router). Tor-projektin juuret johtavat 1990-luvulle jolloin Yhdysvaltain laivaston alkoi kehitellä teknologiaa, jonka avulla pystyttäisiin suojaamaan maan tiedustelupalveluiden yhteydenpito. 2000-luvulle tultaessa Torin kehitys siirtyi laivastolta Tor-projektille, jona se tänä päivänä tunnetaan. Parissa vuosikymmenessä Tor on muovautunut tiedusteluyhteisön yksinoikeudesta työkaluksi, joka on arkipäiväisessä käytössä, niin viranomaisten kuin kotikäyttäjien keskuudessa. (Tor Project 2014a; Tor Project 2014b.)

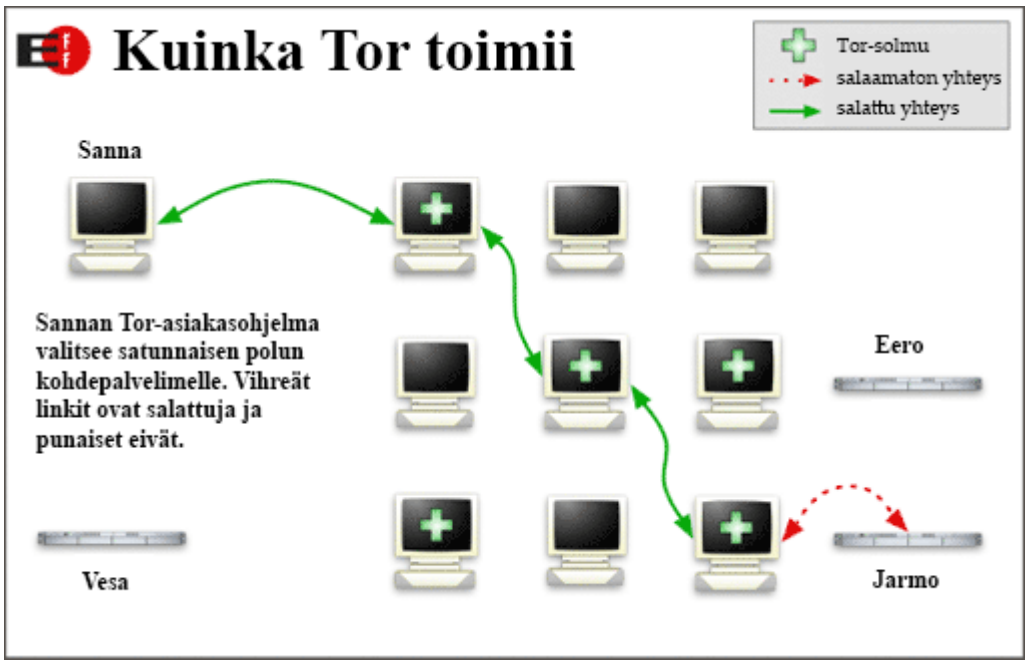
Toria kehittävä ryhmä on voittoa tavoittelematon ja sen toiminnan mahdollistavat lukuisat rahoittajat ympäri maailmaa, joihin ovat lukeutuneet vuosien varrella muun muassa Google ja aikaisemmin luvussa 3 mainittu Electronic Frontier Foundation (EFF). Tämän lisäksi hankkeen toimintaa ovat rahoittaneet tuhannet yksityiset lahjoittajat. (Tor Project 2014d.)

Torin käyttötarkoitukset ovat monet. Kotikäyttäjät pystyvät muun muassa sen avulla viestimään anonyymisti, kiertämään palveluntarjoajien asettamia estoja sekä suojautumaan verkkosivustojen harjoittamalta tietojenkeruulta. Tämän lisäksi se tarjoaa käyttäjille mahdollisuuden päästä käsiksi sisältöön, joka ei olisi mahdollista tavallisimmilla verkkoselaimilla. Torista on myös suurta hyötyä erityisesti toimittajille, jotka pystyvät sen avulla

olemaan yhteydessä toisinajattelijoihin ja ilmiantajiin, joilta he ammentavat informaation artikkeleihinsa. (Tor Porject 2014c.)

6.1.1 Miten Tor toimii?

Kun käyttäjät tavallisesti liittyvät Internet-verkkoon, yhteys otetaan suoraan haluttuun verkko-osoitteeseen. Tor-verkon toiminnan perusideana puolestaan on, että sen läpi kulkeva liikenne hajautetaan kulkemaan kolmen satunnaisen välityspalvelimen kautta. Näistä välityspalvelimista käytetään yleisesti nimitystä *solmu* (node), koska ne ovat ns. solmukohtia, joiden kautta tietoliikenne Tor-verkossa kulkee (Kuva 5). Tällä järjestelyllä pyritään estämään tilanteet, joissa mahdollinen kolmas osapuoli pyrkii seuraamaan tiedonkulkua verkon ylitse. (Tor Project 2014a.)



Kuva 5. Havainnekuva solmujen kautta kulkevasta yhteydestä (Yksityisyydensuoja 2015)

Käyttäjän muodostaessa yhteyden Tor-verkkoon, tämän asiakasohjelma ottaa aluksi yhteyden Tor-hakemistopalveluun, josta noudetaan lista käytössä olevista välityspalvelimista. Tämän jälkeen Tor-ohjelmisto neuvottelee valittujen välityspalvelimien kanssa yksitellen, luoden jokaiselle yhteydelle yksilöidyn salausavaimen, minkä ansiosta kullakin palvelimilla on tiedossa ainoastaan, mistä tieto on tullut ja minne tieto tullaan uudelleen reitittämään. Näin ollen millään palvelimella ei ole tiedossa lähetettävän datan koko reittiä. (Tor Project 2014a.)

Kun ketju käyttäjän, välityspalvelimien ja kohdeosoitteen välille on saatu muodostettua, on dataa mahdollista siirtää luodun yhteyden kautta kymmenen minuutin ajan, jonka jälkeen

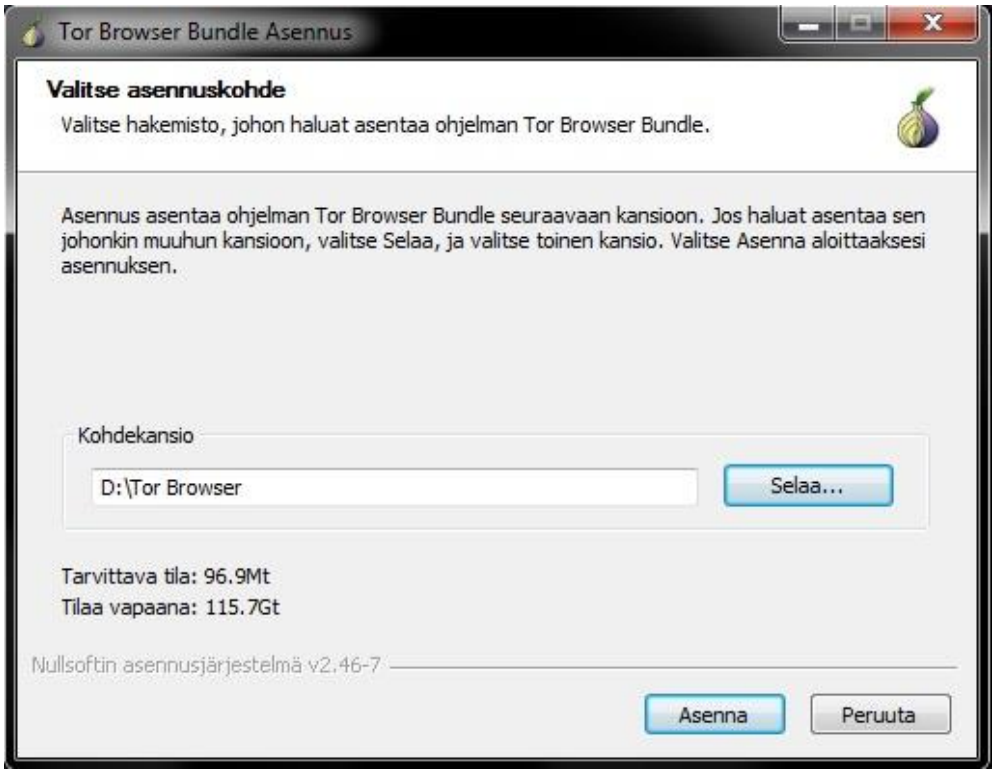
tullaan tarvittaessa luomaan uusi, vastaavanlainen ketju käyttäen eri palvelimia, jotta käyttäjän toimintoja ei pystytä linkittämään toisiinsa (Tor Project 2014a).

6.1.2 Käyttöönotto

Torin käyttöönotto on helppoa ja vaivatonta. Tor Browser on ladattavissa Tor Projectin verkkosivuilta (https://www.torproject.org/projects/torbrowser.html.en) ja sen asentaminen tapahtuu aivan samalla tavoin kuin minkä tahansa muunkin sovelluksen käyttöönotto. Koska tämän työn tarkoituksena oli alun alkaenkin keskittyä pääasiallisesti Windowsin kotikäyttäjiin, niin seuraavat havainnollistavat kuvankaappaukset ovat oleellisia ainoastaan Microsoft Windows käyttäjille.

Ohjelman asennuksen yhteydessä ei tarvitse määritellä kovinkaan monimutkaisia asetuksia. Käyttäjän tulee valita ainoastaan asennuskieli (Kuva 6) sekä kohdekansio (Kuva 7), johon ohjelmisto tullaan asentamaan.

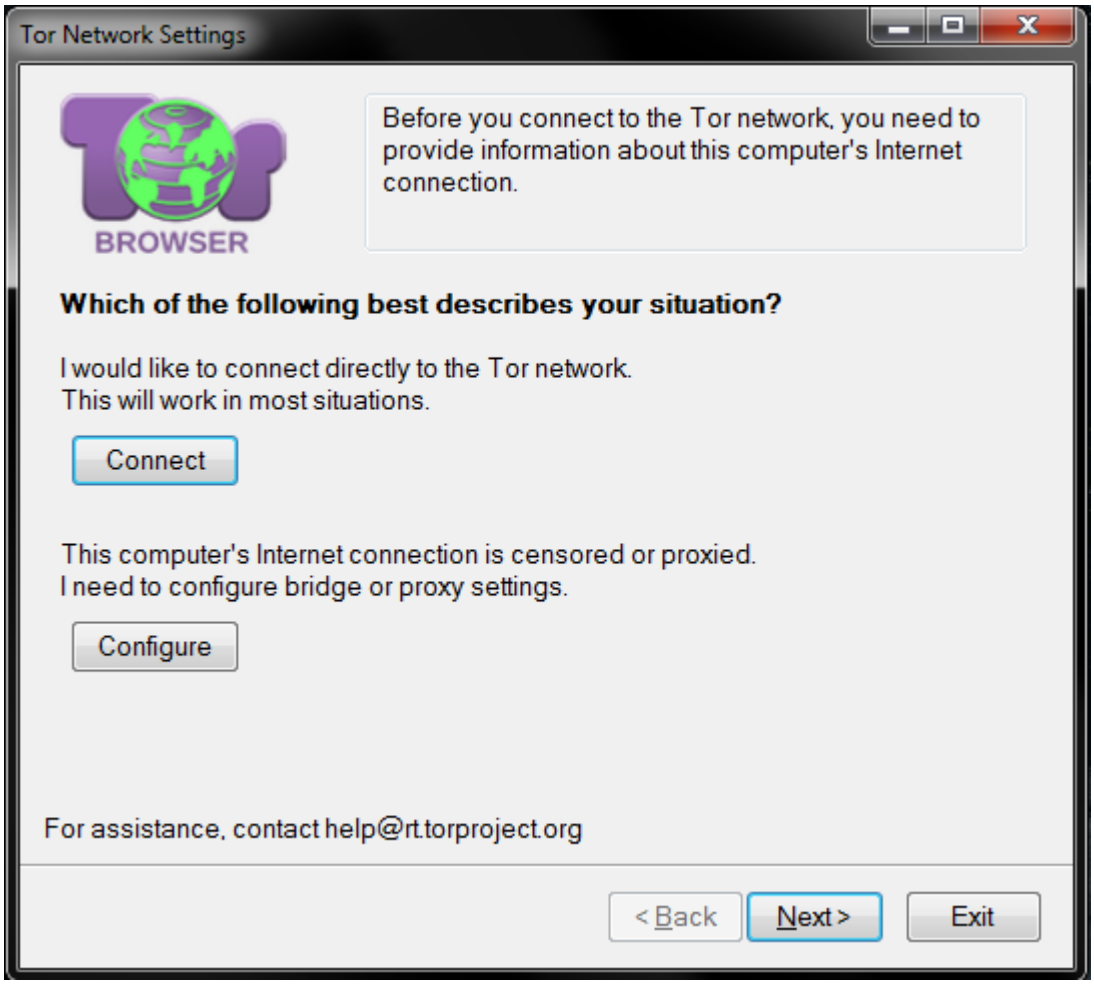
Kuva 6. Asennuskielen valinta



Kuva 7. Asennuskansion valinta

Varsinainen asennusprosessi ei vie kuin hetken ja tämän jälkeen Tor Browser on heti käyttövalmis. Tarvittaessa käyttäjä voi muokata Tor Browserin asetuksia, mutta toistaiseksi tämä ei ole tarpeellista, koska Suomessa Torin käyttöä ei ole rajoitettu. Tämä vaihtoehto olisi tarpeen esimerkiksi Kiinassa, jossa maan hallitus on jo useamman vuoden ajan pyrkinyt estämään Tor-verkon käyttöä. (Tor Project 2014f.)

Aikaisemmissa Tor Browserin versioissa (2.x) selaimen lisäksi pakettiin kuului erillinen ohjauspaneeli Vidalia, jonka avulla käyttäjät pystyivät muokkaamaan Tor-verkkoon liittyviä asetuksia. Kyseinen sovellus on edelleen mahdollista ladata erillisenä pakettina, mutta uusimmissa Tor Browserin versiossa (3.x & 4.x) suurin osa sen toiminnoista on sulautettu Tor Launcherin yhteyteen (Kuva 8). (Tor Project 2014g.)



Kuva 8. Tor-Launcherin avulla käyttäjä muodostaa yhteyden Tor-verkkoon tai vaihtoehtoisesti voi muokata siihen liittyviä asetuksia

6.1.3 Tails

Vaikka tämä työ tehdään silmällä pitäen pelkästään Windows käyttäjiä, ei Toristä puhuttaessa voi sivuttaa Tails nimellä kulkevaa projektia. Se on Debian GNU/Linuxiin pohjautuva käyttöjärjestelmä, jonka perimmäisenä tarkoituksena on turvata käyttäjien yksityisyys ja anonymiteetti. Tämä tapahtuu käytännössä siten, että kaikki Internet-yhteyttä vaativat toiminnot ajetaan Tor-verkon lävitse ja mikäli jostain syystä tämä ei onnistu, kyseiset toiminnot estetään automaattisesti. Tämän lisäksi käyttöjärjestelmä on hyvin poikkeuksellinen myös siitä syystä, ettei sitä tarvitse asentaa lainkaan tietokoneen kiintolevylle vaan se ajetaan suoraan dvd-levyltä, usb-tikulta tai sd-muistikortilta. (Tails 2014.)

Tails on loistava vaihtoehto sellaisille käyttäjille, jotka joutuvat alituisesti käyttämään päätteitä yleisissä tiloissa, kuten esimerkiksi vaikkapa kirjastoissa. Käyttöjärjestelmä tarvitsee toimiakseen ainoastaan tietokoneen fyysistä muistia, joka tyhjenee koneen sammutuksen yhteydestä. Näin ollen käyttäjän toimista ei jää jälkiä tietokoneen tai käyttöjärjestelmän muistiin. (Tails 2014.)

6.1.4 Ongelmakohdat ja muuta huomioitavaa

Voidaanko sitten olla aivan varmoja, että Tor todellakin pitää käyttäjät anonyymeinä? Periaatteessa kyllä, mutta pelkkä ohjelman asentaminen ei kuitenkaan vielä takaa täydellistä identiteetin turvaa, vaan käyttäjien tulee olla entistä tarkkaavaisempia toimintojensa suhteen ja he saattavat joutua myös muuttamaan selailutottumuksiaan. Mainitsemisen arvoista on myös, että vaikka Torin ansiosta käyttäjät pystyvät pitäytymään anonyymeinä, tulee näiden kuitenkin ymmärtää, että tämä koskee ainoastaan sitä Internet-liikennettä, joka on ohjattu kulkemaan Tor-verkon lävitse. (Tor Project 2014e.)

Käyttäjiä kehotetaan myös jättämään Tor Browserin asetukset rauhaan, ellei näillä ole täydellistä tietämystä siitä, mitä he ovat todella tekemässä, koska virheelliset tai vääränlaiset asetukset saattavat tehdä siitä haavoittuvaisen. Lähtökohtaisesti Tor Browserin oletusasetukset on kalibroitu siten, että se takaa käyttäjien pysymisen anonyymeinä. Huomioitavaa kuitenkin on, ettei selaimeen kannata ruveta asentamaan mitään ylimääräisiä liitännäisiä tai lisäosia, koska ne saattavat kiertää Torin tai pahimmassa tapauksessa ne on voitu ohjelmoida paljastamaan käyttäjän IP-osoitteen. (Tor Project 2014e.)

Toria käytettäessä käyttäjien tulee kiinnittää entistä enemmän huomiota selailutapoihinsa. Vaikka tietoliikenne Tor-verkossa on suojattu, voi kohdesivuston salaamattomuus koitua käyttäjän kohtaloksi. Tor Browserin mukana tulee HTTPS Everywhere laajennus, joka automaattisesti pakottaa selaimen käyttämään HTTPS-protokollaa sivustoilla, joissa se on tuettuna. Käyttäjän vastuulle kuitenkin jää huolenpito siitä, että sivustoilla, joilla tämä luovuttaa itsestään edes jossain määrin arkaluontoista informaatiota, on HTTPS-protokolla käytössä (Kuva 9). (Tor Project 2014e.)

Kuva 9. Vihreä lukon kuva kertoo, että yhteys sivustoon on suojattu

Kolmas huomioitava asia, joka poikkeaa huomattavasti tavallisesta verkon käytöstä, koskee Tor-verkon kautta ladattuja tiedostoja. Nyrkkisääntönä on, ettei Tor-verkosta kannata ladata mitään tiedostoja. Vaihtoehtoisesti, jos tätä kautta ladattuja tiedostoja on pakko käsitellä, niin ne tulee avata suljetussa ympäristössä joko käyttämällä tietokonetta, jota ei ole yhdistetty lainkaan verkkoon tai turvautumalla virtualisointiohjelmistoihin kuten esimerkiksi VirtualBoxiin. Tämä varovaisuus johtuu siitä, että ladattavat tiedostot voivat sisältää

haittaohjelmia, jotka voivat vaarantaa käyttäjän identiteetin. Erityistä huomiota vaativat .pdf- ja .doc-päätteiset tiedostot, jotka avataan Tor-verkon ulkopuolella toimivilla ohjelmistoilla ja näin ollen saattavat paljastaa käyttäjän oikean IP-osoitteen. (Tor Project 2014e.)

6.1.5 Lisälaitteet

TorProjectin ympärille on syntynyt viime aikoina lukuisia ulkopuolisten ryhmien itsenäisiä projekteja, joiden tarkoituksena on tuoda käyttäjien ulottuville laitteita, jotka mahdollistaisivat entistä paremmat puitteet verkkoanonyymiyden säilyttämiseksi. Vuoden 2014 lopulla markkinoilla oli tai niille kaavailtiin tulevan lukuisia laitteita, joista mainittakoon InvizBox ja Anonabox. Näistä jälkimmäisen rahoitushanke jouduttiin kuitenkin laittamaan jäihin laitteeseen kohdistuneen kritiikin takia (BBC 2014.), mutta paria viikkoa myöhemmin sama taho kuitenkin aloitti laitteen uudelleen markkinoinnin ja tällä hetkellä näyttäisi, että laitteen ensimmäiset kappaleet olisivat kuluttajien saatavilla helmikuussa 2015.(Indiegogo 2014.)

Kuva 10. Havainnollistava kuva Anonaboxin kytkennöistä (Indiegogo 2014)

Kummankin laitteen perusidea on sama, vaikka ratkaisut eroavat toisistaan hieman. Niiden tarkoituksena on luoda anonyymi Internet-yhteys, jonka turvin käyttäjät voivat huoletta asioida verkossa. Tämä tapahtuu kytkemällä laite kotoa löytyvään reitittimeen tai modeemiin, jonka jälkeen käyttäjä pystyy muodostamaan yhteyden laitteen ja omien laitteiden välille (puhelin, kannettava tietokone, tabletti, pöytäkone) joko langattomasti tai käyttämällä ethernet-kaapelia (Kuva 10). Tämän jälkeen kaikki käyttäjän Internet-liikenne ajetaan Tor-verkon lävitse ilman, että käyttäjän tarvitse asentaa erillisiä sovelluksia tietokoneellensa, minkä johdosta verkkoselaamisen tulisi olla nopeampaa kuin Tor Browserin käyttö. (Indiegogo 2014.)

Kuluttajilla varmasti herää kysymys, etteikö näillä valmistajilla sitten olisi oiva mahdollisuus kerätä laitteiden käyttäjistä informaatiota aivan samalla tavoin kuin luvussa 4.3 mai-

nitut tahot toimivat? Maallikon on mahdotonta tietää tekeekö laite jotain muutakin kuin sen valmistaja väittää. Aika tulee näyttämään ovatko tämän kaltaiset laitteet jonkinlaisia virstanpylväitä tai suunnannäyttäjiä aikakaudelle, jossa verkkoanonyymiuden ihannointi nousee omiin sfääreihinsä ja ne löytyvät poikkeuksetta jokaisesta kotitaloudesta vai ovatko ne vain hetken kestävä villitys ja painuvat pian unholaan.

6.2 Freenet

Freenet on nimensä mukaan ilmainen ohjelmisto, jonka avulla käyttäjät pystyvät anonyymisti jakamaan tiedostoja, selaamaan sekä julkaisemaan omia freesitejaan (joina Freenetin sivustot tunnetaan) ja viestitellä muiden käyttäjien kesken. Freenetin rakenne on hajautettu, jolla on pyritty tekemään sitä vastaan kohdistuvat hyökkäykset vaarattomiksi. Kommunikointi Freenetin solmukohtien välillä on salattu ja reititetty kulkemaan toisten solmujen kautta, mikä tekee tietoliikenteen seuraamisesta erittäin vaikeaa ja antaa vahvan suojan kolmansia osapuolia vastaan. (Freenet 2015a.)

Ohjelmistoa käyttääkseen käyttäjien tulee antaa verkoston käyttöön osa omasta datayhteydestään ja kiintolevytilastaan tiedostojen säilöntää varten. Tiedostot automaattisesti joko tallennetaan tai poistetaan riippuen siitä kuinka yleisessä käytössä ne ovat käyttäjien keskuudessa. Vanha tai vähän käytössä oleva data poistetaan uuden ja suositumman sisällön tieltä. Käyttäjän koneelle tallennettava data on salattua, eikä tällä käytännössä ole mahdollisuutta saada selville, mitä tämän koneelle tallennettu data pitää sisällään. Tämän toiminta periaatteen katsotaan riittävän takaamaan, ettei Freenetin käyttäjiä voida pitää tilivelvollisina siitä millaista tietoa verkossa liikkuu. (Freenet 2015a.)

Freenet on anonyymi vertaisverkko jossa ei ole kiinteitä palvelimia vaan kaikki verkkoon ladattu data salataan ja hajautetaan verkossa olevien koneiden kesken. Hajautetun tiedon säilönnän ansiosta verkkoon ladattu data on aina saatavilla, myös sellaisissa tilanteissa, joissa alkuperäisen tiedoston julkaissut solmu on suljettuna. Tämä ominaisuus erottaa Freenetin muista vertaisverkoista, joissa lähtökohtaisesti tiedoston julkaisseen solmun tulee olla verkossa, jotta haluttuun tiedostoon pääsisi käsiksi. (Freenet 2015b.)

Toinen ominaisuus, joka erottaa Freenetin muista vastaavanlaisista verkoista on darknet-tila, jota käytettäessä käyttäjä on yhteydessä vain sellaisiin käyttäjiin, jotka tämän on luokitellut luotettaviksi. Tällä menettelyllä käyttäjien anonyyminä pysyminen on huomattavasti todennäköisempää ja mahdollistaa silti pääsyn globaaliin verkkoon. Lisäksi tämän toiminnon avulla Freenet on käytettävissä sellaisissa maissa, joissa sen käyttö on estetty valtion toimesta. (Freenet 2015a.)

Freenetin tarpeellisuus tavallisen kotikäyttäjän näkökulmasta riippuu täysin tämän käyttötarpeista. Freenetin kautta käyttäjällä ei ole pääsyä Internetiin eikä näin ollen pysty ottamaan yhteyttä esimerkiksi Facebookin tai Googlen kaltaisiin sivustoihin. Freenetissä on toki vastaavanlaisia palveluita, mutta ennen Freenetin käytön aloittamista käyttäjän kannattaa puntaroida, onko tällä tarvetta aloittaa uusien (kenties turvallisempien) palveluiden käyttö vai pitäytyykö suosiolla entuudestaan tuttujen palveluiden parissa. (Freenet 2015b.)

6.2.1 Hyödyt ja haitat

Hajautettu datan säilöntä tekee tiedostojen jaosta jouhevaa ja yhden solmun kaatuminen ei näin ollen heikennä tietovirran kulkua missään vaiheessa. Lisäksi tiedostojen salauksen ansiosta kenelläkään ei ole tietoa siitä, millaista dataa käyttäjät ovat jakamassa. Tällä pyritään poistamaan käyttäjien tilivelvollisuus, jonka voidaan katsoa olevan, niin hyöty kuin haittakin, koska käyttäjä voi tietämättään levittää arkaluonteista ja laitonta materiaalia, joka on mahdollisesti ristiriidassa tämän eettisten näkemysten kanssa. Freenet tarjoaa vahvan puoleisen anonymiteetin jo perusasetuksillaan, ja mikäli käyttäjällä on riittävästi luotettavia ystäviä, darknet-tilan käyttö näiden ihmisten kanssa tekee käyttökokemuksesta entistä sujuvamman ja turvallisemman. Tiedonjaon lisäksi Freenet tarjoaa käyttäjille alustan anonyymien sivustojen ja viestien julkaisuun.

Freenetin käyttäjän tulee tiedostaa myös sen käyttöön liittyvät mahdolliset riskit, jotka toteutuessaan voivat mahdollisesti paljastaa käyttäjän oikean IP-osoitteen tai henkilöllisyyden sekä millaista tietoa tämä on käsittelemässä. Pääasiallisesti nämä riskit ovat mahdollisia silloin, kun käyttäjä on opennet-tilassa, jossa käyttäjä yhdistetään sattumanvaraisesti johonkin toiseen verkonkäyttäjään. (Freenet 2015c.)

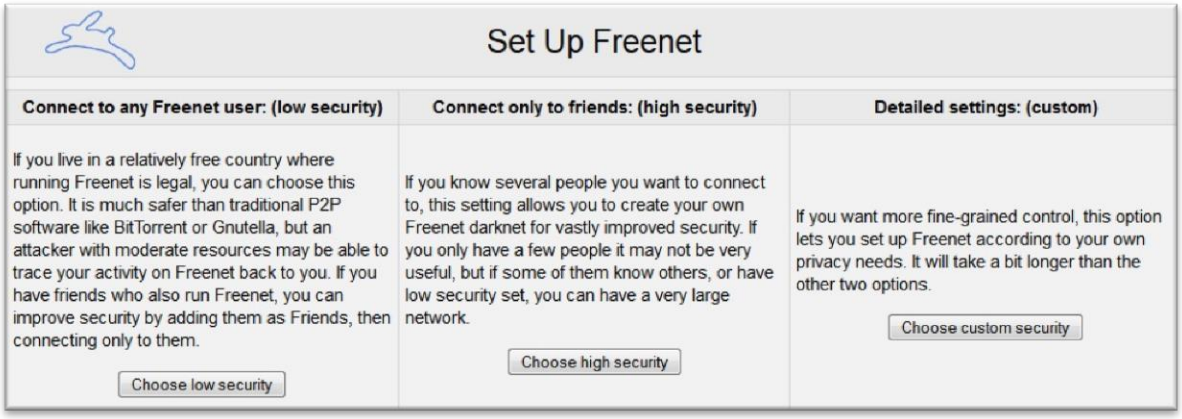
Yhtenä mainitseminen arvoisena epäkohtana Freenetissä on siellä liikkuvan materiaalin laatu. Etenkin lapsiporno ja huumeita välittävien sivustojen olemassaolon tiedostaminen voi olla yksi syy, miksi tavalliset kotikäyttäjä saattavat kiertää Freenetin ja samankaltaiset verkot kaukaa. Korkea anonymiteetin suoja ei tule ilmaiseksi ja tavalliseen verkkosurffailuun tottuneesta käyttäjästä saattaa tuntua, että on palannut viime vuosituhannen puolelle, koska sivujen avaaminen ja tiedonsiirto saattaa tuntua välillä todella hitaalta. Lisäksi Freenetin käyttöönotto ja ymmärtäminen kokemattoman käyttäjän kannalta voi olla alkuun hyvinkin vaikeaa.

6.2.2 Käyttöönotto

Freenetin asentaminen ja käyttöönotto on melko vaivaton toimenpide. Asennustiedosto on ladattavissa Freenet-projektin verkkosivuilta (https://freenetproject.org/). Asennustiedoston lataamisen jälkeen asennus noudattaa Windowsille tavanomaista kaavaa, jossa määritellään asennuksen kannalta oleelliset tiedot (Liite 2).

Kun ohjelmisto on asennettu käyttäjän koneelle ja Freenet käynnistetään ensimmäisen kerran, tulee käyttäjän määritellä Freenetin käyttöä koskevat asetukset. Näihin määrittelyihin kannattaa paneutua, koska ne vaikuttavat merkittävästi Freenetin toimintaan ja suorituskykyyn. Toisaalta kyseisiä asetuksia voi viilailla vielä jälkeenpäin jos tarve vaatii.

Ensimmäiseksi vuorossa on turva-asteen valinta (kuva 11), joka määrittelee yhteyden laadun ja miten ulkopuolisiin uhkiin suhtaudutaan.

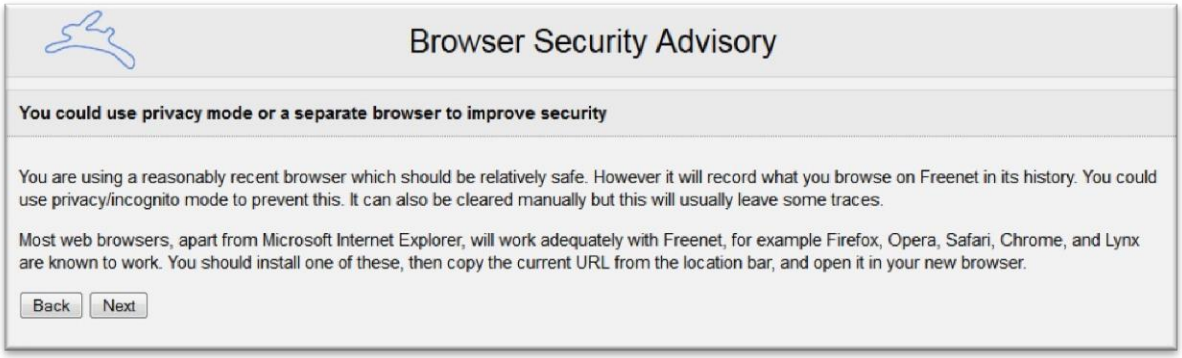


Kuva 11. Turva-asteen määrittely

Paras mahdollinen tilanne uuden käyttäjän näkökulmasta olisi, mikäli tämä tuntisi entuudestaan jo pari muuta Freenetin käyttäjää, jolloin darknet-tilan käyttö olisi mahdollista ensi metreiltä asti. Tällöin ’high security’ olisi sopiva vaihtoehto. Todennäköisempi skenaario on kuitenkin, että uudelle käyttäjälle luontevampi vaihtoehto on ’low security’, joka käytännössä tarkoittaa sitä, että käyttäjä yhdistetään sattuman varaisesti muihin käyttäjiin. Ylläpitäjät kehottavat käyttäjiä verkostoitumaan ja ystävystymään muiden käyttäjien kanssa, jonka jälkeen turva-asetusten korottaminen ja darknet-tilaan siirtyminen opennet-tilan sijasta tekee Freenetin käytöstä nopeampaa ja turvallisempaa.

Turva-asteen valinnan jälkeen selvennetään, ettei Freenettiä tulisi käyttää samassa selaimessa, jolla normaalisti surffaa verkossa (kuva 12). Vaarana on, että käyttäjän selaushistoria voidaan anastaa ja saada sen avulla selville esimerkiksi millaisilla freesiteilla tämä

on vierailut. (Freenet 2015d.) Tässä vaiheessa kannattaa avata siis vaihtoehtoinen selain ja jatkaa asetusten määrittelyjä sen kautta.



Kuva 12. Huomio millä selaimella käytät Freenettiä

Tämän jälkeen vuoroon tulee tietovarastoon koon määrittely, eli kuinka paljon tilaa varataan tietokoneen kiintolevyltä Freenetin käyttöön (Kuva 13). Tietovaraston koko määräytyy sen mukaan kuinka paljon vapaata levytilaa kovalevyllä on. (Freenet 2015f.)

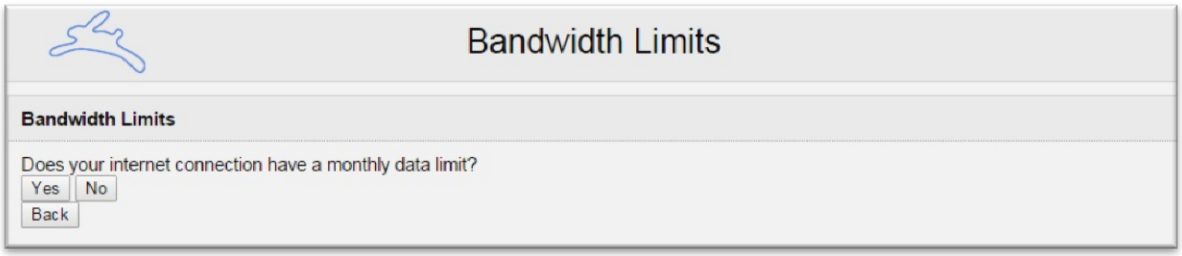
Jos kovalevyllä on vapaata levytilaa yli 20Gt, niin vapaasta levytilasta varataan 5 %
Jos kovalevyllä on vapaata levytilaa yli 10Gt, niin vapaasta levytilasta vartaan 10 %.
Jos kovalevyllä on vapaata levytilaa alle 10Gt, niin levytilasta varataan 512Mt.
Jos kovalevyllä on vapaata levytilaa alle 10Gt, niin levytilasta varataan 512Mt.

Taulukko 1. Tietovaraston koko määräytyy vapaan levytilan mukaan (Freenet 2015f)

Käyttäjä voi halutessaan joko suurentaa tai pienentää luotavan varaston kokoa. Huomioitavaa kuitenkin on, että mitä enemmän tilaa tietovarastolle varaa, sitä sujuvampaa verkonkäytön tulisi olla. Yksittäisen käyttäjän panostus ei välttämättä ole suoranaisesti havaittavissa, mutta mikäli Freenettiä käytetään darknet-tilassa ja kaikki ”piiriin” kuuluvat käyttäjät ovat varanneet merkittävän osan kovalevystään tietovarastolle, on verkon toiminta huomattavasti sujuvampaa kuin oletusasetuksilla. Mainitsemisen arvoista kuitenkin on, että tietovaraston kokoa merkittävämpää on Freenetin käyttöön annettu kaistanleveys. (Freenet 2015f; Freenet 2015g.)

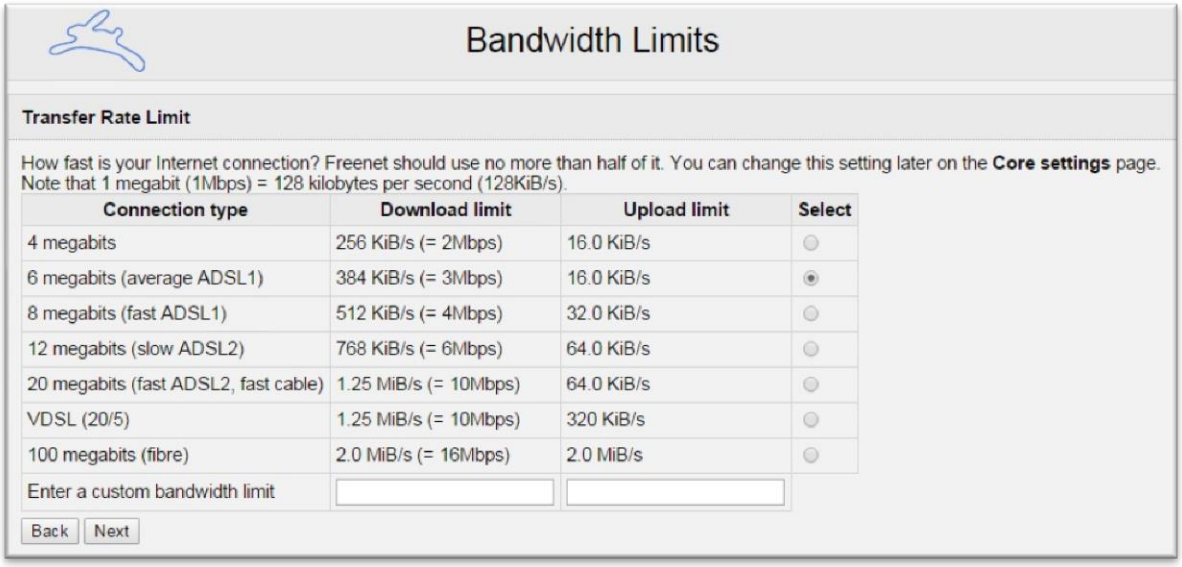
Kuva 13. Tietovaraston koon määrittely

Viimeiseksi vuorossa on kaistanleveyttä koskevat määrittelyt. Käyttäjän tulee asettaa raja sille, kuinka paljon Freenetin käyttöön varataan tämän kaistanleveydestä. Ennen varsinaisten rajojen asettamista käyttäjältä tiedostellaan tämän Internet-yhteyden laatua (Kuva 14). Suurimmalla osalla (suomalaisista) kotikäyttäjistä on tänä päivänä kiinteä laajakaista yhteys, joten kysymys internet-yhteyden datarajoituksesta voi tuntua oudolta.



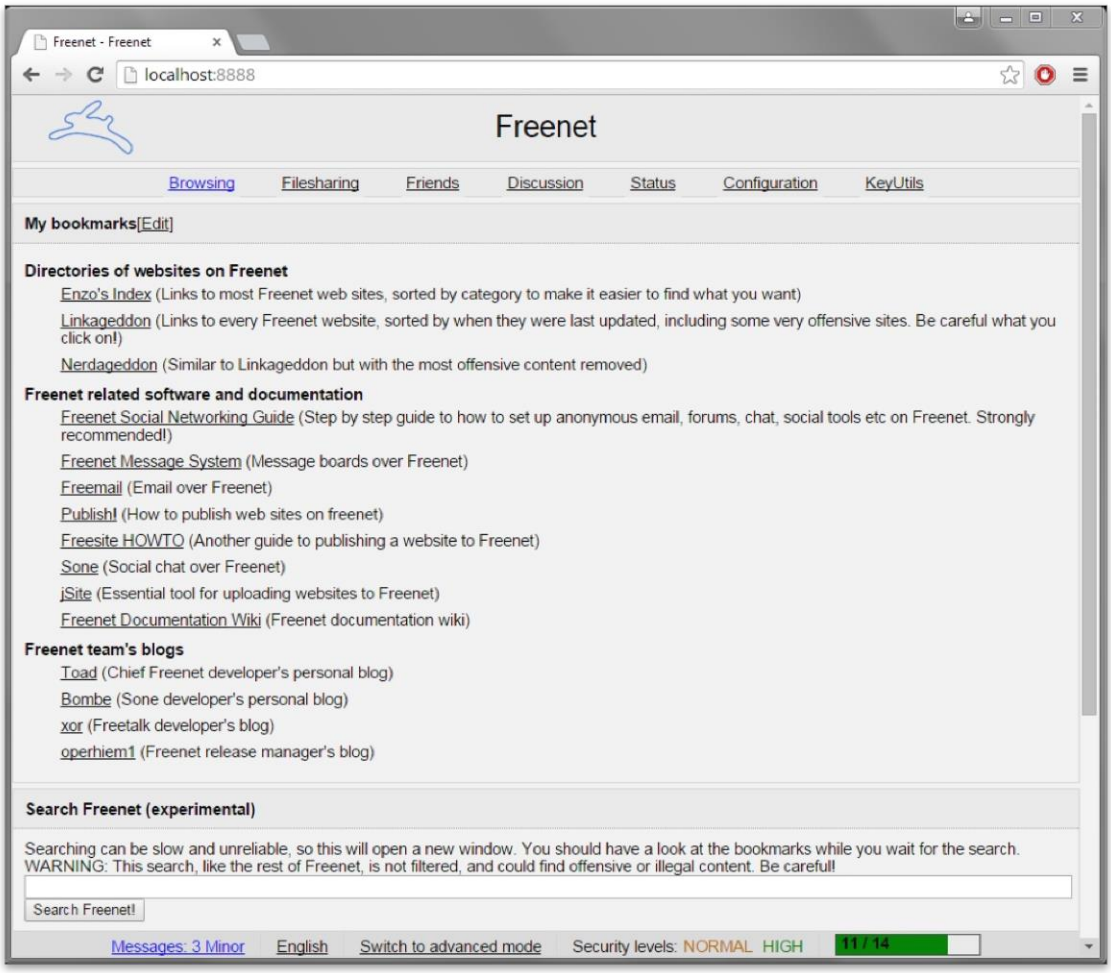
Kuva 14. Kaistanleveyden määrittely 1/2

Tietovaraston luonnin tapaan tässäkin vaiheessa käyttäjän tulee asettaa tietty raja, kuinka paljon Freenetin käyttöön tullaan varaamaan tämän kaistanleveydestä (Kuva 15). Parhaan mahdollisen suorituskyvyn saavuttaakseen Freenetille kannattaa varata riittävästi resursseja, kuitenkaan ylittämättä 50 % rajapyykkiä koko kaistanleveydestä. Jollei ole aivan täyttä varmuutta, kuinka paljon kaistaa tulisi varata, on ehkä turvallisinta aloittaa alhaisista rajoista ja jälkikäteen käydä muokkaamassa niitä, mikäli Freenetin käyttö tuntuu turhauttavan hitaalta. Käyttäjien kannattaa kuitenkin tiedostaa, ettei Freenetin käyttö tule koskaan olemaan yhtä sujuvaa ja nopeaa kuin normaali verkkosurffailu, johtuen sen tarjoamasta anonymiteetin suojasta.



Kuva 15. Kaistanleveyden määrittely 2/2

Tämän jälkeen pakolliset määrittelyt ovat valmiit ja selain siirtyy Freenetin aloitussivulle (Kuva 16).



Kuva 16. Freenetin aloitussivu

Ensimmäiseksi käyttäjä varmasti pistää merkille, ettei Freenetin visuaaliseen ilmeeseen ole panostettu kauheasti ja aloitussivu voi vaikuttaa melko simppeliltä. Aluksi sen toiminta voi myös tuntua hyvin verkkaiselta, joka kuitenkin on täysin normaalia ja tulee nopeutumaan ajan myötä. Jotta Freenetin käyttö olisi mahdollisimman sujuvaa, ylläpitäjät kehottavatkin käyttäjiä pitämään omaa solmua jatkuvasti käynnissä, mikäli tämän vain on mahdollista.

Tarkemmalla silmäilyllä ilmenee, että käyttäjä on saapunut deep webin porteille ja jo Freenetin etusivulla mainitaan arkaluonteisen materiaalin olemassa olosta ja ohjeistetaan käyttäjiä varovaisuuteen. Eettisistä syistä tässä työssä ei käsitellä sen tarkemmin deep webistä löytyvien sivustojen sisältöä.

6.3 Yhteenveto

Anonyymien verkkojen ansioista käyttäjillä on jonkin asteinen mahdollisuus anonyyminä pysymiseen. Jos käyttäjillä on tarvetta oman IP-osoitteen peittelyyn tai normaalit sähköpostipalvelut tuntuvat turvattomilta, niin tässä luvussa käsitellyt ohjelmistot voivat olla tällaisille käyttäjille tervetullut apu. Mikäli käyttäjät ovat aikeissa ruveta käyttämään kyseisiä ohjelmistoja, tulee heidän kuitenkin tiedostaa, että vaikka ne tarjoavat mahdollisuuden anonyymiin asiointiin, eivät ne kuitenkaan suojaa heidän identiteettiään sata prosenttisesti. Aika-ajoin uutisoidaankin tapauksissa, joissa kyseisistä ohjelmistoista on löydetty haavoittuvaisuuksia, joiden johdosta käyttäjien identiteetti on ollut mahdollista selvittää kolmansien osapuolien toimesta. Esimerkiksi Sambuddho Chakravarty pystyi työryhmänsä kanssa murtamaan Torin suojauksen hyväksikäyttämällä reitittimiin sisäänrakennettua tietoliikenneanalyysi-ohjelmistoa (Moon 2014). Vastaavanlaisia tapauksia on lukematto-mia, jotka on suoritettu jonkin valtiollisen tahon toimesta. Esimerkiksi vuoden 2015 tammikuussa Yhdysvaltain kotimaan turvallisuusministeriö pystyi selvittämään Silk Road 2.0:n toiminnassa keskeisesti mukana olleen Brian Richard Farrellin henkilöllisyyden. (Reisinger 2015.)

Tor tarjoaa tällä hetkellä kenties hieman paremman suojan anonymiteetille Freenetin nähden. Tämän lisäksi Toria käytettäessä pystytään myös käsittelemään kaikkea Internetissä tarjolla olevaa dataa, kun taas vastaavasti Freenetissä on saatavilla ainoastaan Freenetin oma sisältö. Toria käytettäessä tulee kuitenkin kiinnittää huomiota omiin selailutottumuksiinsa, koska esimerkiksi sosiaalisen median palveluihin kirjautuminen saattaa paljastaa käyttäjän henkilöllisyyden. Torin suurimmaksi ongelmaksi vaikuttaakin muodostuvan käyttäjien tekemät virheet, joiden johdosta ulkopuoliset tahot saattavat päästä käsiksi käyttäjien henkilökohtaisiin tietoihin. Freenetissä tällaista ongelmaa ei esiinny, mutta käyttäjillä

tulisi olla riittävän suuri luotettavien ystävien piiri, jotta sitä pystyttäisiin käyttämään dark-net-tilassa, mikä tarjoaa erittäin vahvan anonymiteetin suojan. Freenetin etuna on myös se tosiasia, ettei sen käyttöä ole kovinkaan helppo estää, kun taas Torin käyttö on estetty useammassakin eri valtiossa. Kyseinen esto on kyllä mahdollista kiertää, mutta se vaati käyttäjiltä pienimuotoisia ponnisteluja. (Freenet 2015b.)

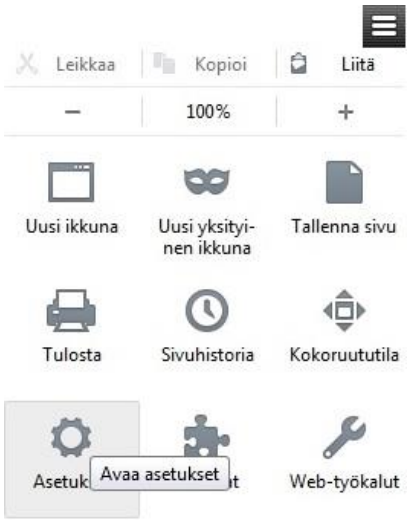
7 Selaimet

Tässä luvussa havainnollistetaan kuinka käyttäjät pystyvät parantamaan verkkoselailu kokemuksiaan ja ehostamaan identiteettinsä suojaa Chrome- ja Firefox selaimissa. Vaikka Internet Explorer (IE) on edelleen hyvin suosittu selain ja varmasti monessa kotitaloudessa se toimii oletusselaimena, niin siitä huolimatta tässä luvussa sitä ei tulla käsittelemään. Omakohtaisesta kokemuksesta voin todeta sen olevan huomattavasti heikommassa asemassa kilpaileviin selaimiin nähden ja sen lukuisat ongelmat takavuosilta edesauttavat tämän päätöksen tekoa. Lisäksi Microsoft ilmoitti hiljattain korvaavansa Internet Explorerin Windows 10:nen julkaisun myötä. (Griffiths & Prigg 2015). Internet Explorerin asetukset ovat kuitenkin hyvin samankaltaiset kuin Chromen ja Firefoxin, joten käytännössä ne takaavat kaikki samat ominaisuudet ja näin ollen IE:n käyttäjien on mahdollista soveltaa tämän luvun ohjeistusta oman selaimensa määrittelyihin.

Mikäli käyttäjillä ei ole tarvetta tai halukkuutta tutustua edellisessä luvussa käsiteltyihin ohjelmistoihin, niin jo pelkästään verkkoselaimen oletusasetuksia muokkaamalla voidaan vaikuttaa huomattavasti siihen informaation määrään, mikä meistä on saatavilla verkossa asioidessamme. Selaimiin on saatavilla myös erinäinen määrä liitännäisiä, jotka tekevät verkkoselailusta entistä jouhevampaa ja parantavat käyttäjien yksityisyyden suojaa. Huomioitavaa kuitenkin on, että jotkin liitännäiset saattavat sisältää haitta- ja vakoiluohjelmia, joten niitä ladatessa kannattaa olla erittäin tarkkaavainen, ettei epähuomiossa lataa epämääräisen julkaisijan tuotoksia.

7.1 Asetusten määrittely ja lisäosat

Firefox

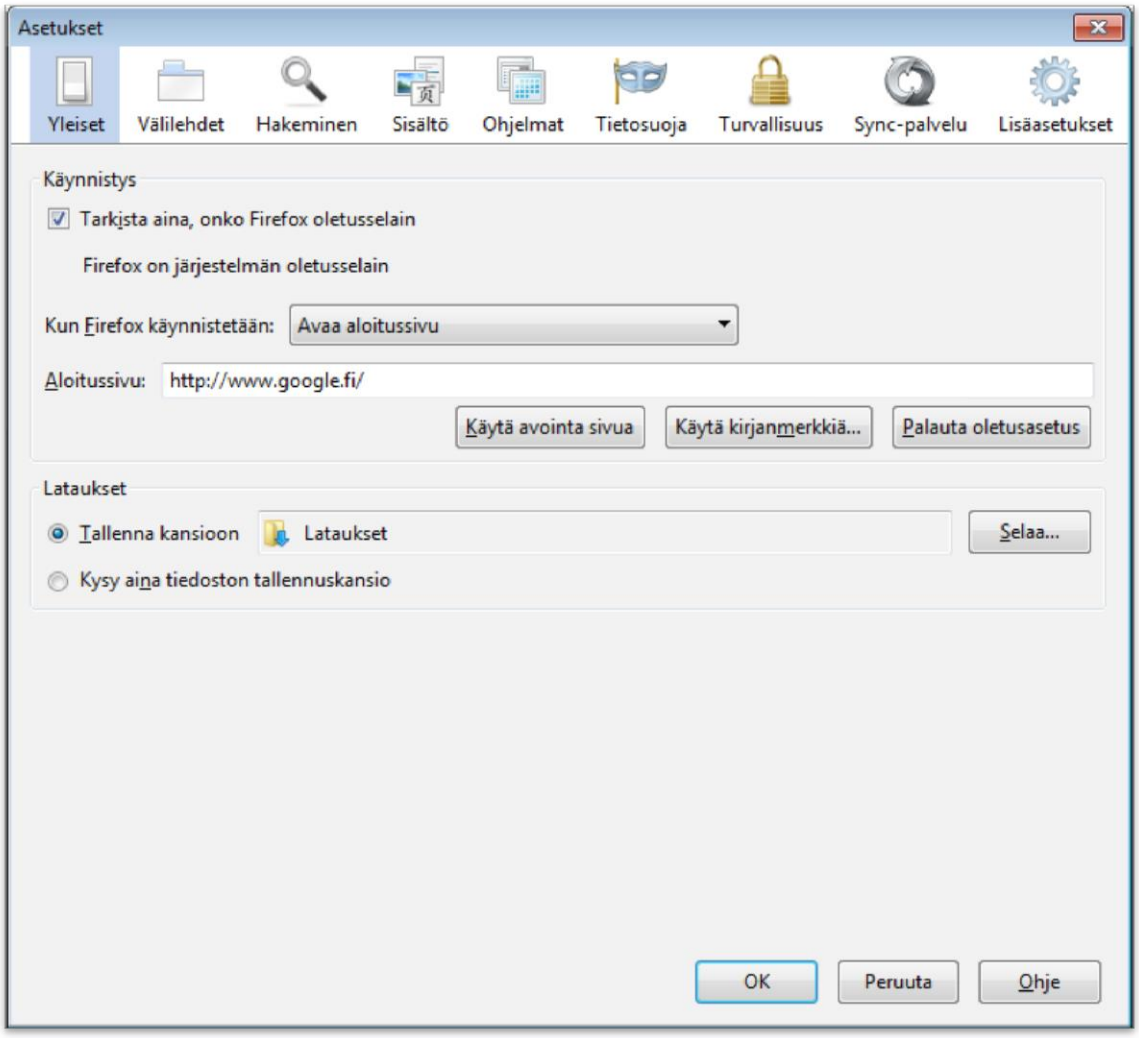


Kuva 17. Avaa Firefoxin asetukset

Firefoxin määrityksiä pääsee muokkaamaan klikkaamalla selainikkunan oikeassa yläreunassa olevaa valikkokuvaketta ja valitsemalla vaihtoehdon Asetukset (Kuva 17).

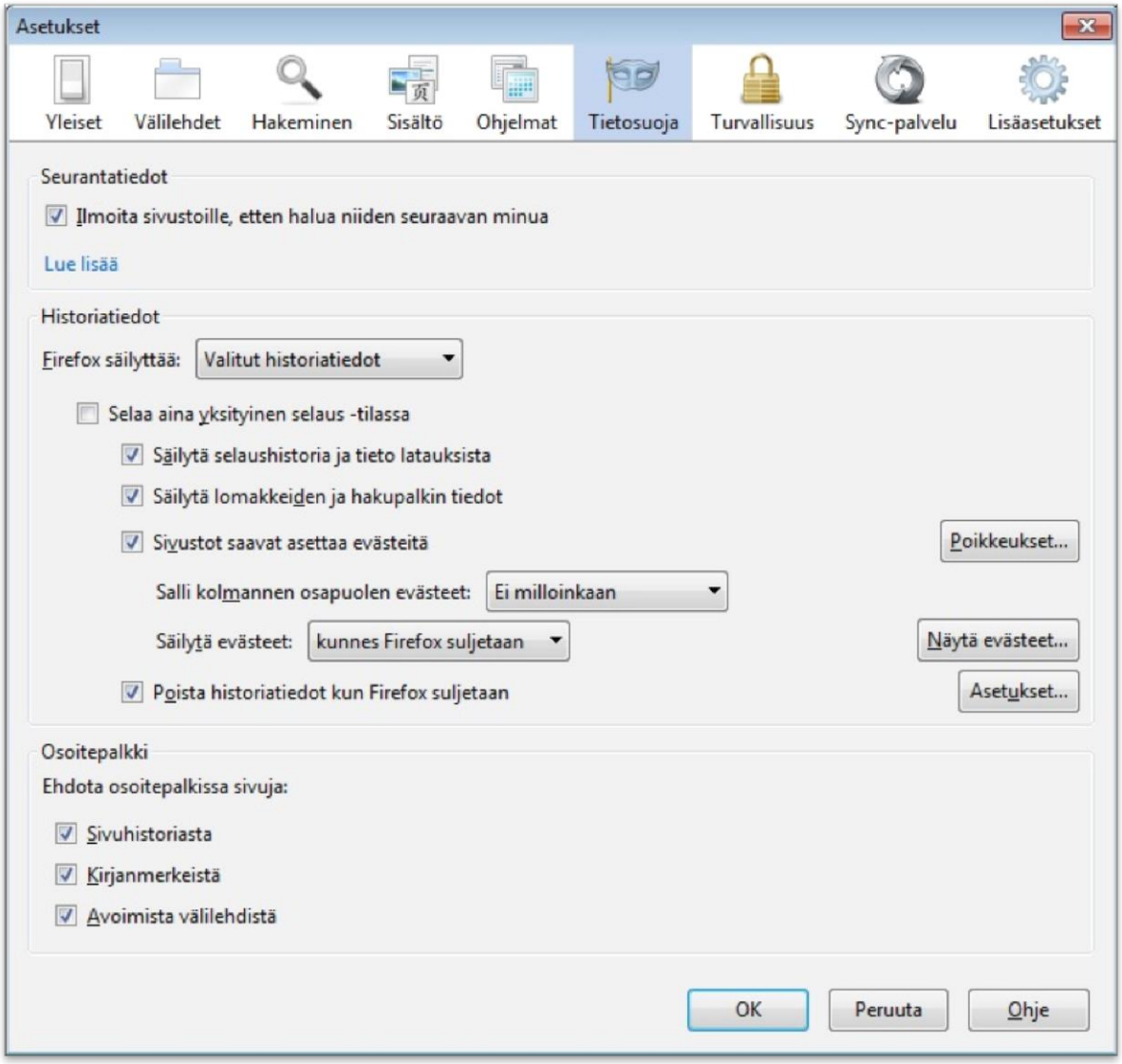
Asetukset on myös mahdollista saada näkyviin navigoimalla valikkopalkista löytyvään Työkalut pudotusvalikkoon, josta löytyy valinta Asetukset. Mikäli valikkopalkki ei syystä tai toisesta ole näkyvissä, saa sen esille joko klikkaamalla ikkunan yläreunaa hiiren oikealla painikkeella ja valitsemalla ilmestyvästä valikosta Valikkopalkki tai vaihtoehtoisesti saman toiminnon voi myös suorittaa painamalla Alt-näppäintä.

Tämän jälkeen ruudulle aukea kokonaan uusi ikkuna (Kuva 18), josta löytyvät kaikki selainta koskevat asetukset, omille välilehdilleen jaoteltuina. Tällä erää ei ole tarkoitus paneutua kaikkiin mahdollisiin selaimen asetuksiin vaan ainoastaan tutustua Tietosuoja- ja Turvallisuus-välilehdiltä löytyviin asetuksiin.



Kuva 18. Asetukset-ikkunan aloitusnäkymä

Tietosuoja-välilehdellä (Kuva 19) kannattaa tarkistaa ensimmäiseksi, että Seurantatiedot osiossa on valintamerkki seuraamisen estotoiminnon kohdalla. Käytännössä tämä tarkoittaa sitä, että Firefox tiedottaa kaikille vierailemillesi sivustoille, näiden mainostajille ja sisällöntuottajille, ettet halua niiden seuraavan selaamistasi. Seuraamalla käyttäjien selailua nämä tahot saavat haltuunsa arvokasta dataa ihmisten selailutottumuksia, joita soveltamalla sitten osaavat kohdistaa tietynlaisia mainoksia ja palveluita kyseiselle käyttäjälle. Kannattaa kuitenkin huomioida, ettei verkkosivustojen tarvitse noudattaa tätä pyyntöä, joten on hyvinkin mahdollista, että selaamista seurataan näistä toimenpiteistä huolimatta. (Mozilla 2015a.)



Kuva 19. Firefoxin Tietosuoja-välilehti

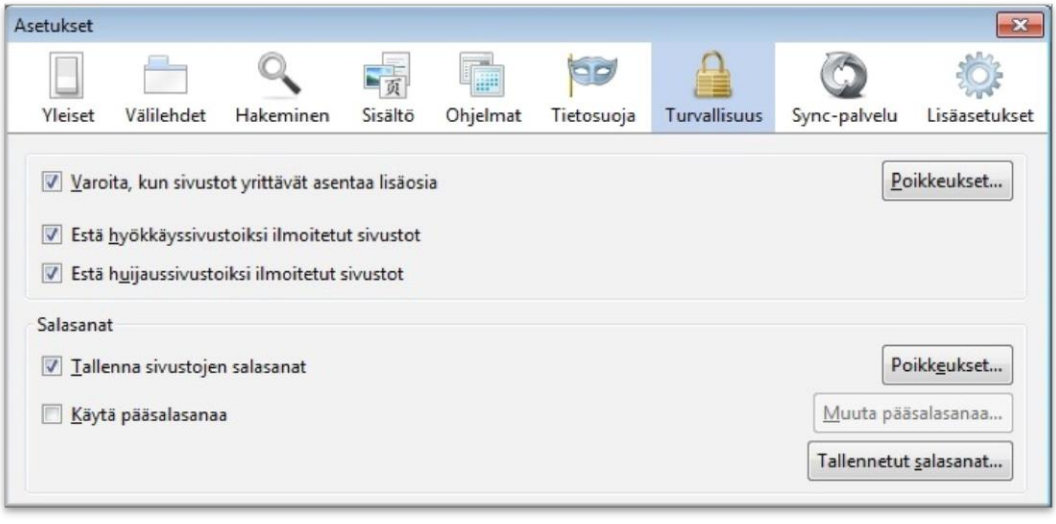
Samaiselta välilehdeltä löytyy myös historiatietoja käsittelevä osio, josta voidaan valita kolmesta vaihtoehdosta itselleen sopivin vaihtoehto. Nämä valinnat määrittelevät sen, miten Firefox säilyttää selaimen historiatietoja.

Firefox käyttää oletuksena Täydellisten historiatietojen säilyttämistä. Tämän asetuksen muuttaminen on suositeltavaa, mikäli käyttäjä haluaa parantaa yksityisyyden suojaansa, koska muutoin selain kerää kaikki sivu-, lataus-, lomake- ja hakuhistoriatiedot sekä evästeet sivuilta, jolla käyttäjä on vieraillut.

Ei mitään historiatietoja – vaihtoehto takaa, ettei selaimen muistiin jää mitään evästeitä tai lomaketietoja. Näin ollen selain on jokaisella käynnistyskerralla kuin uusi eli sen muistissa ei ole mitään historiatietoja edellisestä sessiosta. Tämä on oiva vaihtoehto tilanteisiin, joissa samaista tietokonetta/käyttäjätiliä käyttää useampi eri henkilö. Suositeltavaa kuitenkin on, että jokaisella tietokoneen käyttäjällä olisi oma yksilöity käyttäjätilinsä, jolloin jokaisella koneen käyttäjällä olisi automaattisesti myös oma Firefox – profiilinsa. Näin ollen muilla koneen käyttäjillä ei olisi mahdollisuuksia nähdä toistensa historiatietoja tai mahdollisuuksia päästä kirjautumaan verkkosivustoille muiden tunnuksilla selaimeen tallennettujen salasanojen avulla.

Kolmantena vaihtoehtona on Valitut historiatiedot, jonka valitseminen antaa käyttäjälle vapaamman mahdollisuuden spesifioida historiatietoja koskevia asetuksia ja määrityksiä. Tämä on kaikin puolin hyvä vaihtoehto kotikäyttöön, koska sen avulla käyttäjät voivat halutessaan määritellä, mitkä historiatiedot tullaan poistamaan selaimen sulkeutumisen yhteydessä tai kuinka pitkään evästeitä säilytetään. Tarkempi listaus kaikista yllä mainituista vaihtoehdosta ja niiden ominaisuuksista löytyvät liitteistä. (Liite 3).

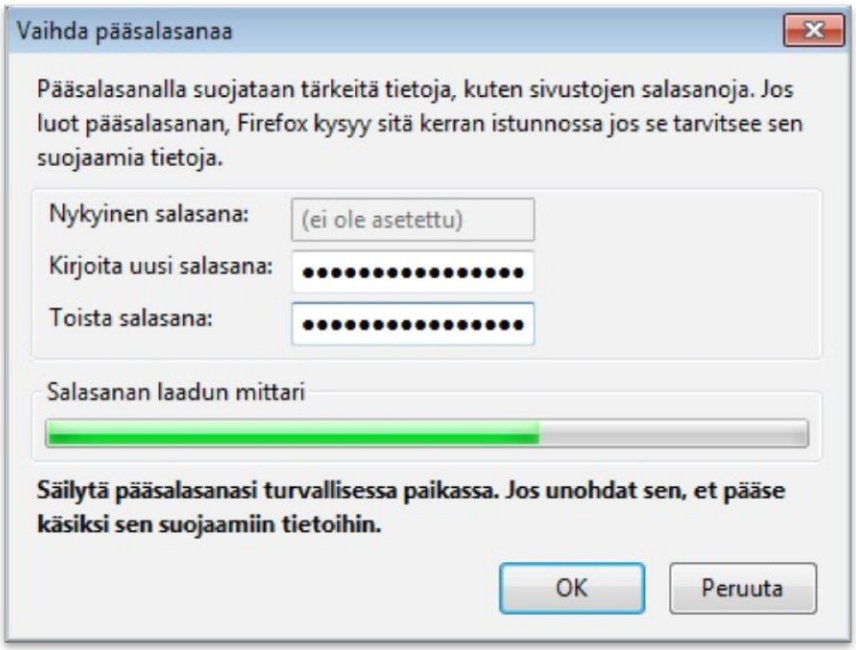
Turvallisuus-välilehdeltä (Kuva 20) tulee tarkistaa, että kolmesta ensimmäistä vaihtoehdosta löytyy merkintä, että kyseiset asetukset ovat käytössä. Pääsääntöisesti näiden tulisi olla jo automaattisesti päällä, mutta mikäli näin ei ole, kannattaa puuttuvat määrittelyt ottaa käyttöön.



Kuva 20. Turvallisuus-välilehti

Hyökkäys- ja huijaussivustoja koskevien estojen lisäksi turvallisuus-välilehdeltä voidaan määritellä salasanojen tallentamiseen liittyvät asetukset. Käyttäjät voivat halutessaan poistaa oletusasetuksena olevan vaihtoehdon, että selain tallentaa sivustoille annetut salasanat. Mikäli tämä ominaisuus halutaan pitää päällä, on suositeltavaa ottaa pääsalasana käyttöön, koska kaikki selaimen muistiin tallennetut salasanat on helppo käydä tarkistamassa selaimen asetuksista: Työkalut > Asetukset > Turvallisuus > Tallennetut salasanat.. > Näytä salasanat. Eli käytännössä jos pääsalasanaa ei ole asetettu, niin tallennetut salasanat ovat vapaasti nähtävillä ja kirjautumista verkkosivustoille ei kontrolloida millään tavoin.

Pääsalasana otetaan käyttöön klikkaamalla *Käytä pääsalasanaa*, jonka jälkeen avautuu uusi ikkuna, johon syötetään haluttu salasana kahdesti (Kuva 21). Pääsalasanaa tullaan tiedustelemaan kertaalleen jokaisessa istunnossa silloin, kun käyttäjä ensimmäisen kerran pyrkii kirjautumaan tallennettua salasanaa käyttäen. Tämän lisäksi sitä tarvitaan myös tilanteissa jos halutaan tarkastella selaimen muistiin tallennettuja salasanoja.

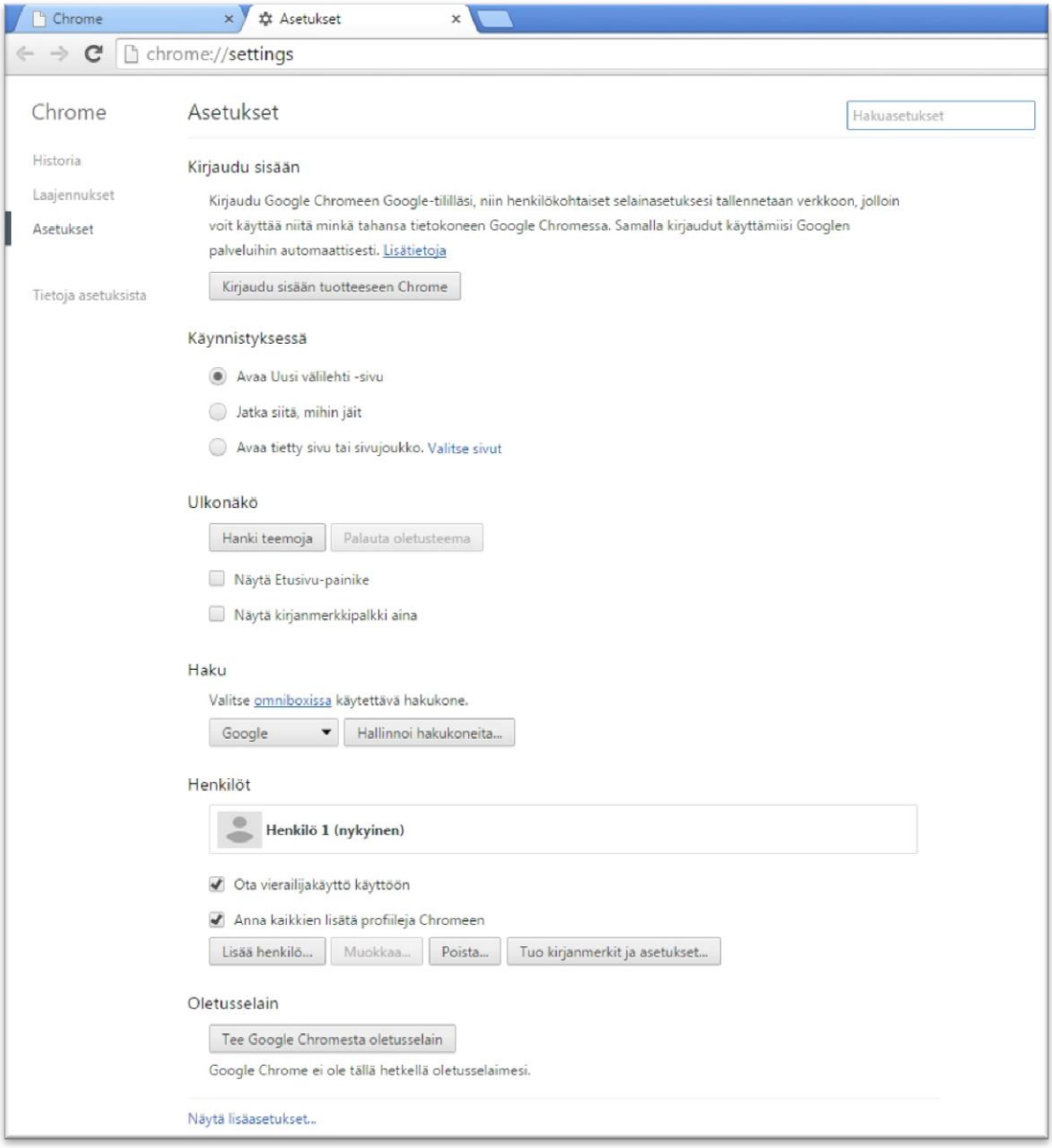


Kuva 21. Pääsalasanan luominen

Google Chrome

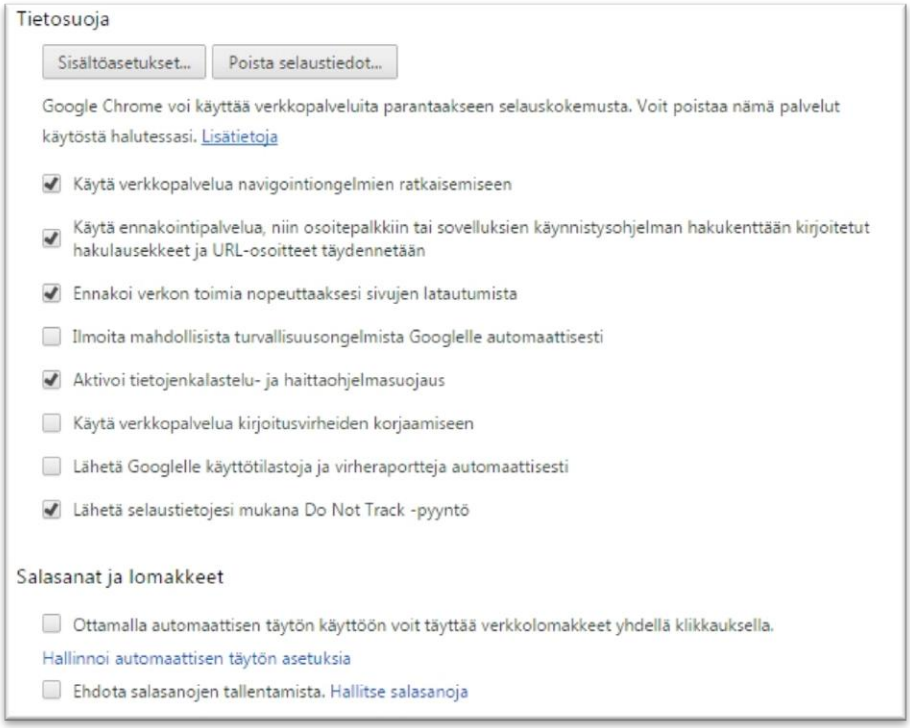
Chromen asetukset löytyvät klikkaamalla selainikkunan oikeassa yläreunassa olevaa painiketta ja valitsemalla Asetukset, jonka jälkeen avautuu uusi välilehti (Kuva 22). Chromen asetusmäärittelyt ovat kaikki listattuna samalle sivulle eikä käyttäjien näin ollen tarvitse poukkoilla välilehdeltä toiselle löytääkseen haluamansa asetuksen toisin kuin Firefoxissa. Toisaalta yksilöityjen välilehtien ansiosta selain ikkuna on siisti ja selkeämpi, kun kaikki

määrittelyt eivät ole samalla sivulla. Chromessa on myös mahdollisuus käyttää hakutyökalua, joka nopeuttaa huomattavasti haluttujen asetuksien löytymistä.



Kuva 22. Chromen perusasetukset

Chromessa käyttäjien yksityisyyttä koskevat asetukset ovat huomattavasti laajemmat ja mutkikkaammat kuin Firefoxissa, joten niiden sisäistämiseen ja määrittämiseen saa kulutettua huomattavan paljon aikaa. Nämä asetukset löytyvät Chromen lisäasetuksista, jotka saa näkyville klikkaamalla Asetukset-välilehden alalaidassa olevaa valintaa Näytä lisäasetukset… Lisäasetuksiin kuuluu noin kymmenkunta kategoriaa, joista yksityisyysasetuksien määrittelyt löytyvät Tietosuoja otsikon alta (Kuva 23).



Kuva 23. Tietojasuoja- ja salasanamäärittelyt

Firefoxin tapaan Chromessakaan Do Not Track –pyyntö ei ole oletuksena käytössä, joten tämä on ensimmäinen kohta, joka käyttäjien kannattaa muuttaa. Turvallisuuden maksimoimiseksi käyttäjien kannattaa myös poistaa käytöstä salasanojen tallentaminen ja lomakkeiden automaattinen täyttö. Chromessa salasanat on mahdollista nähdä selkokielisenä, mikäli Windows-käyttäjätilille ei syystä tai toisesta ole asetettu salasanaa.

Laajemmat määrittelyt saadaan auki klikkaamalla Sisältöasetukset… -painiketta, jotka ovat huomattavasti tarkemmat ja laajemmat kuin Firefoxissa. Sisällöltään ne ovat kuitenkin hyvin pitkälti samankaltaiset.

7.2 Lisäosat

Verkkoselaimiin on saatavilla valtavasti erilaisia lisäosia ja liitännäisiä joiden avulla voidaan parantaa ja tehostaa verkkoselaamisen laatua. Selainta ei kannata kuitenkaan kuormittaa aivan turhaa näillä ylimääräisillä lisäosilla, koska ne voivat aiheuttaa satunnaisia komplikaatioita, minkä johdosta selain saattaa kaatua ja vaatia uudelleen käynnistämistä. Lisäksi jotkin lisäosat ja liitännäiset saattavat sisältää haitta- tai seurantaohjelmia, joten niitä ladattaessa ei kannata toimia harkitsemattomasti. Suositeltavaa olisi tehdä pientä taustatutkimusta kyseisestä lisäosasta tai liitännäisestä ja lukea muiden käyttäjien tekemiä arvosteluja, jolleivät ne ole entuudestaan tuttuja.

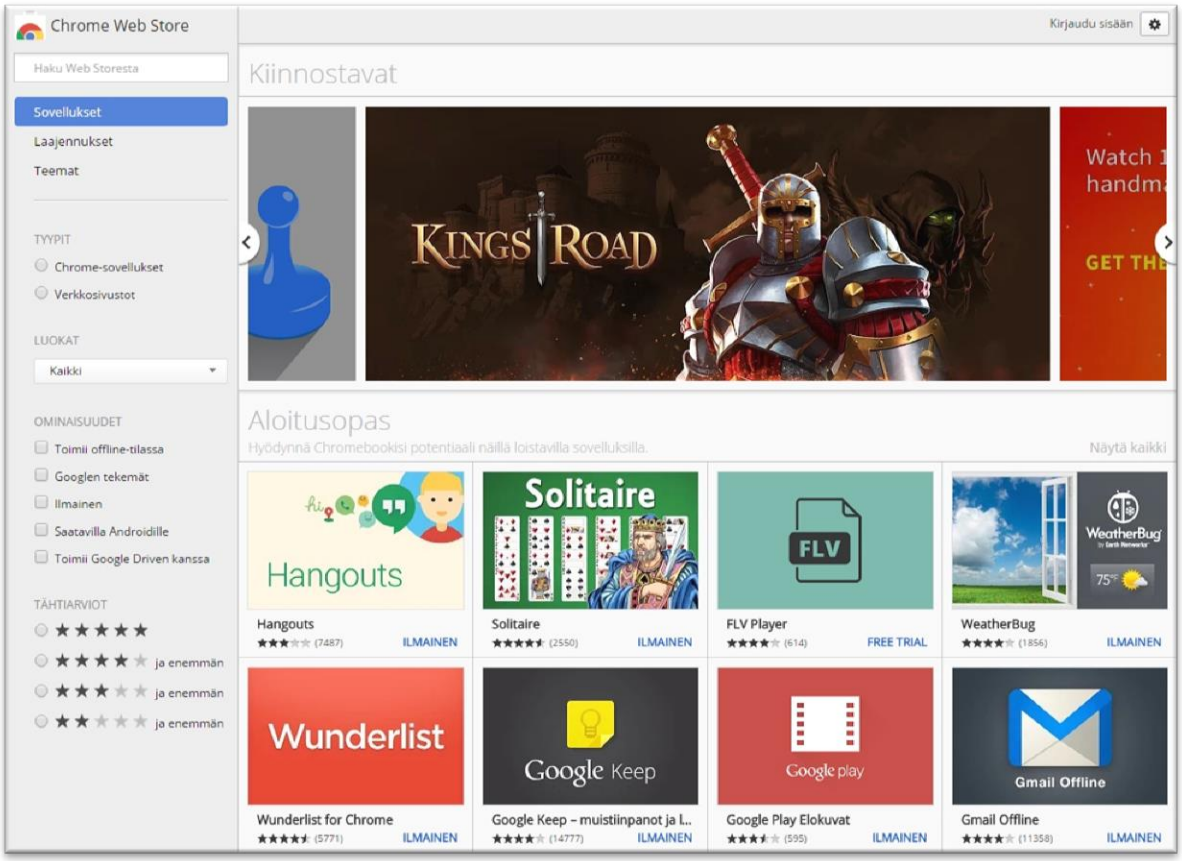
Suositeltavia lisäosia niin Firefoxiin kuin Google Chromeenkin käytettäviksi ovat AdBlock Plus ja HTTPS Everywhere joiden avulla käyttäjät pääsevät hyvin alkuun. AdBlock Plus on selainlaajennus, jonka avulla käyttäjät pystyvät estämään verkkosivustoilla esiintyviä mainoksia näkymästä. HTTPS Everywhere on puolestaan hyvä vaihtoehto, kun halutaan parantaa verkkoselailun turvallisuutta ja pyrkiä varmistamaan, etteivät henkilökohtaiset tiedot päädy ulkopuolisten haltuun. Halutessaan käyttäjät voivat asentaa lisäosia ja laajennuksia lukuisiin erilaisiin tarkoituksiin. Tarjolla on esimerkiksi kielityökaluja joiden avulla käyttäjät voivat nopeasti kääntää vieraskielisiä sanoja ja lauseita omalle äidinkielelleen tai halutessaan voivat muokata selaimen käyttöliittymää ja sen ulkonäköä omanlaisekseen.

Firefoxissa lisäosien hallintaan pääsee käsiksi samasta valikosta, josta myös selaimen asetuksia koskevat määrittelyt löytyivät. Lisäosien hallintaikkuna on selkeä ja helppokäyttöinen (Kuva 24). Lisäosia pystyy etsimään omatoimisesti sanahaulla tai selailemalla kategorisoituja listoja suositummista laajennuksista ja lisäosista.

Kuva 24. Firefoxin lisäosien hallinta

Google Chromessa lisäosien ja laajennuksien hallintaan pääse helpoiten navigoimalla itsensä selaimen asetuksiin (Katso kuva 22) ja klikkaamalla vasemmasta paneelista Laajennukset. Vaihtoehtoisesti Laajennukset -ikkuna saadaan suoraan näkyville syöttämällä osoiteriville chrome://extensions/. Laajennuksien aloitusnäkymässä on listattuna ainoastaan ne lisäosat ja liitännäiset, jotka selaimessa on käytössä. Mikäli uusia laajennuksia

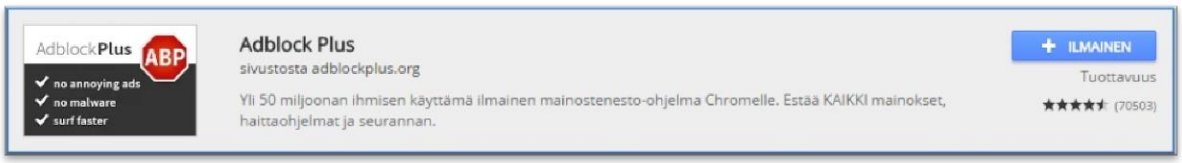
halutaan asentaa, tulee käyttäjän klikata ikkunan alalaidasta olevaa vaihtoehtoa Hanki lisää laajennuksia ja Chromen Webstore avautuu uuteen välilehteen (Kuva 25).



Kuva 25. Chrome Web Storen aloitusnäkymä

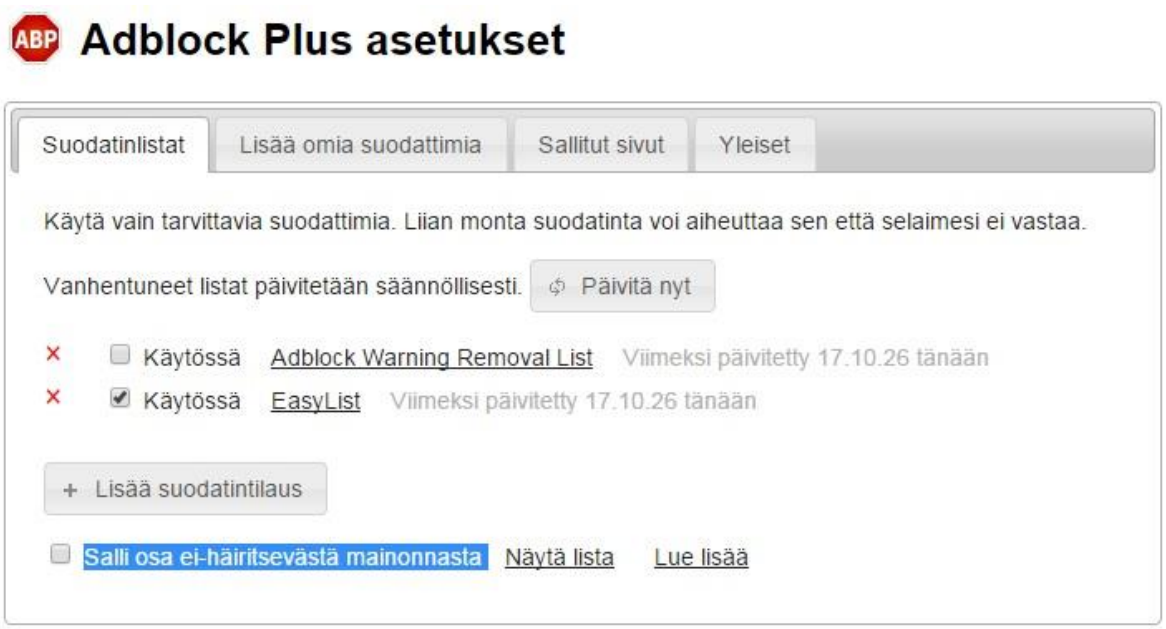
Chromessa lisäosia ja liitännäisiä pystyy etsimään paljon kattavammin ja kyseinen ominaisuus toimii Firefoxiin verrattuna myös huomattavasti sujuvammin, mikä sinänsä on aivan odotettavaa, sillä onhan kyseessä Googlen kehittämä selainohjelma.

Lisäosien ja liitännäisten asentaminen on nopeaa ja vaivatonta. Kun haluttu laajennus on löytynyt, käytetään tässä esimerkkinä vaikka aikaisemmin mainittua AdBlock Plussaa (Kuva 26). Asennus tapahtuu klikkaamalla + ILMAINEN –painiketta, minkä jälkeen käyttäjän tulee vielä vahvistaa uuden laajennuksen asentaminen.



Kuva 26. Adblock Plus Chromen Web Storessa

Itse asennusprosessi ei kestä kuin hetken, minkä jälkeen laajennus on käyttövalmis. Asennettujen laajennuksien asetuksia päästään muokkaamaan Laajennukset – ikkunan kautta. Adblock Plussan kohdalla on suositeltavaa käydä muuttamassa asetus suodatinlistan käytössä, johon listattu lukuisia sivustoja joiden mainokset on luokiteltu ei-häiritseviksi ja näin ollen niitä ei myöskään oletuksena estetä (Kuva 27).



Kuva 27. Poista asetus ei-häiritsevän mainonnan sallimisesta

7.3 Evästeet

Eväste (cookie) on käyttäjän tietokoneelle tallentuva tiedosto, joka sisältää informaatio käyttäjästä ja tämän toiminnasta. Kun ollaan aikeissa siirtyä evästeitä käyttävälle sivustolle, verkkosivu pyytää selainta tallentamaan evästeet käyttäjän laitteelle. Tämä edellyttää kuitenkin käyttäjän suostumuksen, minkä lisäksi evästeiden ja niiden käyttötarkoitus on selvitettävä käyttäjälle. Evästeet voivat olla istuntokohtaisia, jolloin ne tuhoutuvat, kun palvelun käyttö lopetetaan. Vaihtoehtoisesti niitä voidaan säilyttää laitteella pysyvästi, niin kauan kunnes niille määritelty aikaraja umpeutuu tai ne poistetaan käyttäjän toimesta. (Viestintävirasto 2014.)

Evästeiden avulla voidaan kerätä esimerkiksi:

- Käyttäjän IP-osoite, kellonaika, käytetyt sivut ja selain tyyppi
- Mistä verkko-osoitteesta käyttäjä on tullut kyseiselle verkkosivulle
- Miltä palvelimelta käyttäjä on tullut verkkosivulle
- Mistä verkkotunnuksesta käyttäjä on tullut verkkosivulle.

Taulukko 2. Evästeet paljastavat käyttäjän selailutottumukset (Viestintävirasto 2014)

Jotkin verkkosivustot saattavat vaatia evästeiden käytön, jotta ne toimisivat moitteettomasti. Yleisesti ottaen evästeet ovat täysin vaarattomia ja hyödyksi käyttäjille. Niiden ansiosta verkkoselaaminen onnistuu sujuvammin, minkä johdosta käyttäjien ei tarvitse esimerkiksi täyttää kaavakkeisiin samoja tietoja useaan otteeseen. Valitettavasti evästeiden käyttöön liittyy myös joitain ongelmia, koska niiden avulla pystytään seuraamaan käyttäjien selailu tottumuksia, mikä saattaa tuntua joistain käyttäjistä hyvinkin epämiellyttävältä. Tämä on mahdollista kolmansien osapuolten suosimilla seurantaevästeillä, joita käytetään kohdennetussa verkkomainonnassa. Seurantaevästeiden avulla mainonnantarjoajat tietävät millaisia mainoksia tietyt käyttäjät ovat nähneet ja pystyvät näin ollen kohdistamaan näille sellaisia mainoksia, jotka vastaavat käyttäjien selailutottumuksia (F-Secure).

7.4 Yhteenveto

Mozilla Firefox ja Google Chrome ovat tällä hetkellä kaksi varteenotettavinta verkkoselainta, mistä syystä jommankumman käyttäminen olisikin erittäin suositeltavaa. Toisaalta on ymmärrettävää, että mikäli on tottunut käyttämään joitain muuta selainta, kuten Internet Exploreria voi selaimen vaihtaminen alkuun tuntua hankalalta. Yleisesti ottaen kaikki selaimet kuitenkin tarjoavat osapuilleen samat ominaisuudet ja suojamekanismit, joten loppujen lopuksi selaimen valinta kulminoituu siihen, mitä vaihtoehtoa käyttäjä itse suosii.

Asetukset Firefoxin ja Chromen välillä, eivät sisältönsä puolesta eroa toisistaan kovinkaan paljoa, mutta molempiin tutustuneena Mozillan Firefoxin määrittelyt tuntuivat, jossain määrin helpommilta ja valikot hieman selkeämmiltä. Tähän totta kai vaikuttaa se tosia, että Firefox on toiminut oletusselaimen asemassa jo useamman vuoden ajan. Jotta selainten toimintoja ja käyttäjäystävällisyyttä olisi voitu vertailla puolueettomasti, niin projektin aikana olisi pitänyt myös suorittaa jonkun asteinen kyselytutkimus, jolla olisi kyetty kartoittamaan käyttäjien mieltymyksiä ja mielipiteitä.

Selainten asetuksia muuttamalla pystytään vaikuttamaan huomattavasti siihen tiedon määrään, joka käyttäjistä on mahdollista saada selville. Huomioitavaa kuitenkin on, että vaikka selaimissa tänä päivänä on mahdollista käyttää Incognito-tilaa eli yksityistä selaamista, niin se ei kuitenkaan takaa käyttäjille anonymiteettiä, vaan esimerkiksi Internet-palveluntarjoajat pystyvät edelleen seuraamaan millä verkkosivulla käyttäjät vierailevat. Incognito-tila ei myöskään vaikuta millään tavoin erilaisten vakoiluohjelmien toimintaan. (Mozilla 2015b.)

8 Muut menetelmät

Käyttäjillä on myös muitakin mahdollisuuksia jo aikaisemmin esitettyjen menetelmien lisäksi, joilla voidaan parantamaan oman yksityisyyden säilymistä verkossa asioidessa. Tällaisia ovat esimerkiksi anonyymien hakukoneiden ja virtuaalisen erillisverkkon käyttö.

Anonyymit hakukoneet

Käyttäjät voivat esimerkiksi suorittaa verkkohakunsa Googlen sijaan anonyymeillä hakukoneilla, jotka eivät Googlen tapaan kerää ja tallenna tietoja käyttäjistään. Verkko on pullollaan tämänkaltaisia hakukoneita, mutta kenties eniten näkyvyyttä on kerännyt DuckDuckGo niminen projekti, joka on ollut käytettävissä vuodesta 2008 lähtien. Kehittäjiensä mukaan kyseinen hakukone eroaa Googlesta ja muista hakukoneista sen suhteen, että se asettaa ennen kaikkea käyttäjien yksityisyyden etusijalle, eivätkä ulkopuoliset tahot näin ollen saa esimerkiksi tietoonsa, millaisia hakusanoja käyttämällä käyttäjät ovat kyseiselle sivustolle päätyneet. Anonyymejä hakukoneita käytettäessä on kuitenkin huomioitavaa, että siinä missä se voittavat yksityisyyden varjelussa ne häviävät hakutuloksissa, eivätkä näin ollen voi välttämättä taata yhtä kattavia ja tarkkoja hakutuloksia kuin esimerkiksi Google. (DuckDuckGo.)

VPN

VPN eli Virtual Private Network on tekniikka, joka mahdollistaa turvallisen ja luotettavan yhteyden muodostamisen Internetiin tai mihin tahansa muuhunkin julkiseen verkkoon. VPN-yhteyttä käytettäessä ulkopuolisilla ei ole mahdollisuutta anastaa istunnossa käsiteltävää dataa. Tämä on pyritty takaamaan käyttämällä kahta erillistä suojamekanismia. Ensinnäkin yhteyden data salataan siten, että jos jostain syystä ulkopuolinen taho pääsee käsiksi lähetettävään informaatioon, ei se ole luettavassa muodossa kolmannen osapuolen hallussa. Dataa ei myöskään pureta luettavaan muotoon ennen kuin lähettävä osapuoli on varmistanut siitä, että viestin on vastaanottanut taho jolle se alun perin oli tarkoitettukin. Tämän lisäksi data kulkee verkossa kyseistä toimenpidettä varten luodun tunnelin kautta, minkä johdosta tätä protokollaa kutsutaankin tunneloinniksi. Tunnelointiprotokollia on kuitenkin useita erilaisia ja tietyt VPN-palveluntarjoajat saattavat käyttää eri menetelmiä. Perus ideana kuitenkin on, että vertauskuvallisen tunnelin avulla pystytään sulkemaan pois kaikki ylimääräiset järjestelmät, eivätkä ulkopuoliset tahot näin ollen pääse yhteyden väliin. (VPN Ground.)

VPN tarjoaa myös varteenotettavan anonymiteetin suojan, koska yhteyden ansiosta käytettävissä on lukuisia eri IP-osoitteita, joiden avulla todellinen IP-osoite pystytään naamioimaan lukuisia kertoja ennen kuin data saapuu käyttäjän koneelle. Näin ollen ulkopuolisen tarkkailijan on mahdotonta tietää käyttäjän todellista osoitetta. (VPN Ground). Käyttäjillä on mahdollisuus valita lukuisista VPN-palveluntarjoajista itselleen sopivin. Tarjolla on maksullisten palveluiden lisäksi myös ilmaisia vaihtoehtoja, mutta kuten minkä tahansa muunkin palvelun kohdalla, maksulliset vaihtoehdot tahtovat olla huomattavasti laadukkaampia ja turvallisempia.

9 Yhteenveto

Tämän opinnäytetyön tarkoituksena oli perehtyä verkkoanonymiteettiin, sitä sivuaviin käsitteisiin ja ilmiöihin tavallisten kotikäyttäjien näkökulmasta, minkä lisäksi pyrittiin kartoittamaan ohjelmistoja ja menetelmiä, joiden avulla käyttäjät pystyisivät parantamaan oman yksityisyytensä suojaa Internetissä asioidessaan. Työssä tutustuttiin Torin ja Freenetin lisäksi siihen, miten selainasetuksia muuttamalla voidaan vaikuttaa käyttäjien yksityisyyteen sekä nimettiin muita varteenotettavia menetelmiä anonymiteetin säilyttämiseksi.

Tor ja Freenet antavat käyttäjille hyvän anonymiteetin suojan, mutta käyttäjien ei kuitenkaan kannata luottaa näihin ohjelmistoihin täysin sokeasti, koska niissäkin on heikkoutensa. Yksityisyyden kannalta ne kuitenkin tarjoavat huomattavan edun normaaliin verkkoselaamisen nähden, kunhan käyttäjät vain jaksavat noudattaa ylläpitäjien laatimia ohjeita. Anonymiteetti ei kuitenkaan tule aivan ilmaiseksi, sillä tiedonsiirtonopeus näitä ohjelmia käytettäessä putoaa huomattavasti tavallisiin menetelmiin verrattuna, mikä saattaa osittain vaikuttaa siihen, minkä vuoksi ne eivät ainakaan vielä ole saavuttaneet valtaväestön suosiota. Mikäli käyttäjät eivät kuitenkaan pidä Torin tai Freenetin kaltaisten ohjelmistojen käyttöä itselleen mieluisena vaihtoehtona, voidaan yksityisyyden suojaa pyrkiä parantamaan myös huomattavasti yksinkertaisemmin keinoin. Verkkoselainten asetuksia muokkaamalla ja niihin ladattavien lisäosien avulla käyttäjät voivat esimerkiksi estää verkkosivuilla esiintyvät mainokset ja minimoida itsestään saatavilla olevien tietojen määrän.

Verkkoanonymiteetin aiheuttamat lieveilmiöt ja niiden vaikutukset käyttäjiin ja koko yhteiskuntaan ovat korostuneet selvästi viimeisten vuosien aikana, johon myös hallinnolliset tahot ovat havahtuneet. Uusia lakialoitteita ollaan ajamassa lävitse niin Euroopassa kuin USA:ssakin, jotka läpi mennessään saattaisivat vaikuttaa huomattavasti käyttäjien yksityisyyteen ja sananvapauteen Internetissä. Tieto siitä, että verkossa asiointia ruvettaisiin valvomaan entistä systemaattisemmin, saattaisi muuttaa käyttäjien selaustottumusten lisäksi pysyvästi myös Internetin tarjoamia palveluita ja niiden toimintamalleja. Yksi mahdollinen skenaario voisi olla, ettei suosimiamme Internetpalveluita pystyisi tulevaisuudessa enää käyttämään nimettömästi ja näin ollen käyttäjien väliset keskustelut ja muu asioiminen ei olisi enää yhtä vapaata ja avointa.

Toisaalta jonkin asteinen muutos olisi ihan suotavaa ottaen huomioon, kuinka paljon erilaista häiriköintiä ja rikollista toimintaa verkossa on havaittavissa. Väistämätön tosiasia kuitenkin on, että tavalliset verkonkäyttäjät tulevat olemaan kuitenkin häviävä osapuoli oli tilanne tulevaisuudessa sitten mikä tahansa. Uusilla tiukemmilla lakiuudistuksilla pyritään kitkemään rikollisuutta ja ehkäisemään mahdollisten terrori-iskujen toteutuminen, mutta

eittämättä tämä tulisi vaikuttamaan myös lainkuuliaisiin kansalaisiin. Valvonnan tiukentuessa on selvää, että laittomuuksia suunnittelevia käyttäjiä ja ryhmittymiä jäisi entistä enemmän kiinni, mutta samalla kasvaisi myös todennäköisyys sille, että viranomaiset saattaisivat tehdä karkeita virhearviointeja, minkä seurauksena lainkuuliaisia käyttäjä saatettaisiin tuomita syyttöminä.

Myös alati kehittyvä teknologia tulee vaikuttamaan väistämättä käyttäjien yksityisyyteen lähitulevaisuudessa. Aikaisemmin käyttäjillä oli mahdollisuutena kirjautua erilaisiin palveluihin ainoastaan kyseistä sivustoa varten vasten luodulla käyttäjätunnus - salasana yhdistelmällä. Sittemmin menetelmät ovat muuttuneet ja nykyään käyttäjät voivat kirjautua esimerkiksi Google-tilillään lukuisiin eri palveluihin. Kärjistetyin skenaario on, että jos muutos jatkuu samankaltaisena, niin lähitulevaisuudesta voidaan olla tilanteessa, jossa käyttäjien kaikki toimintaa tapahtuu yhden käyttäjätilin kautta. Tällöin käyttäjien yksityisyys ja anonymiteetti ovat entistä alttiimmassa asemassa paljastua, mikäli tilitiedot päätyvät vääriin käsiin. Toisaalta on mahdotonta ennustaa tulevatko verkossa käytettävät tunnistautumismenetelmät muuttumaan vai säilyvätkö ne ennallaan, koska tuskin vielä vuosituhannen alussa kukaan osasi aavistaa, että pankkitunnuksilla ja mobiilivarmenteilla kirjautuminen olisi käsite tulevaisuudessa.

9.1 Jatkoehdotukset

Koska tätä opinnäytetyötä ei suoritettu minkään yrityksen toimeksiantona, ei siitä näin ollen myöskään ole hyötyä suoranaisesti millekään yksittäiselle taholle vaan tarkoituksena oli luoda informatiivinen tietopaketti aiheesta kiinnostuneille. Mahdollisesti tästä työstä voisi olla myös apua muille opiskelijoille, jotka eivät ole saaneet toimeksiantoa opinnäytetyötään varten tai eivät muutoin ole löytäneet mielenkiintoista aihetta projektilleen.

Projektin edetessä ilmeni useita varteenotettavia aiheita, joista voisi hyvinkin saada kehiteltyä uuden opinnäytetyön aiheen. Ensinnäkin tämän työn ulkopuolelle rajattu mobiilipuoli on yksinään jo niin laaja aihe, että siitä saisi aivan varmasi sovellettua hyvän ja kehityskelpoisen projektin. Kyseisessä työssä voisi tutkia vaikkapa erilaisia tapoja joilla pystyttäisiin kommunikoimaan anonyymisti tai vaihtoehtoisesti jos opiskelijalta löytyy enemmänkin koodaustaustaa, niin oman applikaation luominen, joka mahdollistaisi jonkin asteisen anonyymin toiminnon, voisi olla mielenkiintoinen aihe niin tekijälleen kuin lukijoille.

Itselläni kävi myös mielessä opinnäytetyötä suunniteltaessa, että verkkoanonymiteettiä olisi voinut lähesty myös paljon teknisemmästä näkökulmasta ja keskittyä pelkästään testaamaan erilaisia ohjelmistoja ja vertailemaan niiden ominaisuuksia ja käyttäjäystävälli-

syyttä. Tällöin teoriatausta olisi jäänyt melko vähälle huomiolle, koska pääpaino olisi ollut niin sanotusti testaamisessa ja vertailussa.

Verkkoanonymiteettiin ja sitä sivuaviin aiheisiin tutustuessani mieleeni puolestaan juolahti tuon tuosta mahdollisia opinnäytetyön aiheita, joista välttämättä kaikki eivät kuitenkaan olisi suoranaisesti sopivia tietojenkäsittelyn opiskelijoille. Esimerkiksi yksityisyyden lainsäädäntöä käsittelevästä opinnäytetyöstä saisi varmasti hyvin kattavan ja laajan kokonaisuuden jos vain olisi mielenkiintoa perehtyä erinäisiin lakeihin ja meneillään oleviin lakialoitteisiin eri puolilla maailmaa.

Tässäkin työssä jonkin verran käsiteltyä internet-kiusaamista voisi lähteä tutkimaan joko kiusaajien tai uhrien näkökulmasta. Otollinen kohderyhmä tutkimukselle olisivat yläasteikäiset nuoret, mutta tällöin nuorten vanhemmilta tarvittaisiin suostumus nuorten osallistumisesta tutkimukseen, joka puolestaan saattaisi olla merkittävä kompastuskivi projektin onnistumiselle.

Tämän lisäksi luvussa 5 käsiteltyihin mainonnan ja markkinoin eri muotoihin voisi tutusta vaikkapa opiskelija, joka työskentelee jossain suuremman kokoluokan yrityksessä. Opiskelija voisi vaikkapa kartoittaa millaisia mainonnan muotoja yrityksessä harjoitetaan ja miten niitä voitaisiin jatkossa parantaa. Tämän tosin edellyttäisi sitä, että opiskelija saisi toimeksiannon kyseisestä yrityksestä.

9.2 Työprosessi ja oma oppiminen

Työn alkumetreiltä asti oli selvää, että aiheen rajauksen kanssa tulisi olla erittäin varovainen ja harkita huolella, mitkä aihealueet tultaisiin rajaamaan projektin ulkopuolelle, koska muutoin työstä olisi saattanut tulla liian laaja ja epäselvä kokonaisuus. Käyttäjäkeskeinen lähestymistapa valittiin siitä syystä, ettei tarkoituksena ollut tehdä aiheesta pelkkää kirjallisuuskatsausta, vaan pyrkiä jollain tavoin myös konkreettisesti havainnollistamaan niitä tapoja ja menetelmiä, joilla käyttäjät pystyisivät itse vaikuttamaan oman identiteettinsä suojaan.

Työ eteni melko verkkaisesti koko projektin ajan, koska mitään varsinaista takarajaa työlle ei tullut asetettua. Ainoa vaatimus oli, että sen tulisi valmistua viimeistään kevääseen mennessä. Alun perin hyvin optimistisena suunnitelmana oli saada opinnäytetyö valmiiksi jo syyslukukauden (2014) aikana. Valitettavasti kirjoittaminen ei kuitenkaan sujunut niin jouhevasti, että projekti olisi valmistunut jouluun mennessä. Toinen seikka, joka ei vastannut aivan odotuksia, oli lähteiden hakuun käytettyjen työtuntien määrä. Ennen projektin

aloittamista mietitytti löytyisikö aiheesta riittävästi taustamateriaalia, mutta toisin kuitenkin kävi, kun ongelmaksi muodostuikin, että lähteitä oli tullut kerättyä lopulta aivan liikaa ja niitä täytyi ruveta karsimaan.

Projektia aloittaessa verkkoanonymiteetin tarpeellisuus tuntui itsestään selvyydeltä, mutta erinäisiä tutkielmia, blogeja ja keskustelufoorumeja luettuani näkemykseni aiheesta alkoi hieman muuttua. Omien yksityistietojen vaaliminen verkossa asioidessa on totta kai tärkeää, mutta herää kysymys, tarvitseeko tuiki tavallisten käyttäjien nähdä kaikki se vaiva, jolla saavutetaan näennäinen anonymiteetti. Toisin sanoen onko käyttäjien tarpeellista ladata erillisiä ohjelmistoja, joilla pyritään esimerkiksi peittämään oman tietokoneen IP-osoite vai riittäisikö pelkästään järkevien ja turvallisten toimintatapojen noudattaminen tavallisessa kotikäytössä?

Henkilökohtaisesti voin todeta, etten tule muuttamaan omia toimintatapojani kovinkaan paljoa sen johdosta, mitä tämän projektin aikana olen oppinut ja sisäistänyt. Ehkä huomattavin muutos tulee olemaan sen suhteen, kuinka paljon tietoja itsestäni luovutan jatkossa erilaisten palveluiden ja sivustojen käyttöön. Lisäksi olen alkanut kiinnittämään entistä enemmän huomiota esimerkiksi sosiaalisessa mediassa tapahtuvaan mainontaan ja pyrkinyt selvittämään, mistä syistä tiettyjä mainoksia kohdennetaan juuri minulle.

Kaiken kaikkiaan opinnäytetyöprosessin teko on ollut mielenkiintoista ja palkitsevaa. Erityisesti omien vahvuuksien ja heikkouksien tunnistaminen työn edetessä on ollut tärkeää tulevaisuuden kannalta, koska jatkossa osaan kiinnittää entistä enemmän huomiota niihin osa-alueisiin, joista löytyy vielä parannettavaa.

Lähteet

Arena, K. 2005. Bush says he signed NSA wiretap order. Luettavissa: http://edition.cnn.com/2005/POLITICS/12/17/bush.nsa/. Luettu 15.12.2014.

BBC 2014. Kickstarter cancels plan to make anonymising router. Luettavissa: http://www.bbc.com/news/technology-29652773. Luettu 8.1.2015.

Bullying Statistics 2013. Cyber Bullying Statistics. Luettvissa: http://www.bullyingstatistics.org/content/cyber-bullying-statistics.html. Luettu 21.1.2015.

Channel 4 2013. Snowden delivers Channel 4's Alternative Christmas Message. Luettavissa: http://www.channel4.com/news/edward-snowden-nsa-gchq-whistleblower-surveillance-spying. Luettu 06.11.2014.

DuckDuckGo. Privacy. Luettavissa: https://duckduckgo.com/privacy. Luettu 9.4.2015.

Euroopan unioni 2011. Attitudes on Data Protection and Electronic Identity in the European Union, s. 6. Luettavissa: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf. Luettu: 6.11.2014.

FBI 2008. The New Phenomenon of ‘Swatting. Luettavissa: http://www.fbi.gov/news/stories/2008/february/swatting020408. Luettu 30.3.2015.

Federal Trade Commission 2014. Luettavissa: Data Brokers – A Call for Transparency and Accountabilityhttp://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf. Luettu: 3.12.2014.

Fight for the Future 2014. Luettavissa: https://www.fightforthefuture.org. Luettu 2.12.2014.

Freenet 2015a. What is Freenet? Luettavissa: https://freenetproject.org/whatis.html. Luettu 22.1.2015.

Freenet 2015b. Frequently Asked Questions Luettavissa: https://freenetproject.org/faq.html#tor. Luettu 22.1.2015.

Freenet 2015c. Luettavissa: https://wiki.freenetproject.org/Opennet_attacks. Luettu 26.1.2015.

Freenet 2015d. Frequently Asked Questions. Luettavissa: https://freenetproject.org/faq.html#browser. Luettu 27.1.2015.

Freenet 2015e. Connecting to Freenet. Luettavissa: https://freenetproject.org/connect.html. Luettu 27.1.2015.

Freenet 2015f. Understand Freenet. Luettavissa: https://freenetproject.org/understand.html. Luettu 28.1.2015.

Freenet 2015g. Frequently Asked Questions. Luettavissa: https://freenetproject.org/faq.html#donate-lot. Luettu 28.1.2015.

F-Secure. Tracking cookie. Luettavissa https://www.f-secure.com/sw-desc/tracking_cookie.shtml. Luettu 16.4.2015.

Gibbs, S. 2013. 'Waterproof iPhone' ad hoax tricked users into destroying their handsets. The Guardian. Luettavissa: http://www.theguardian.com/technology/2013/sep/26/waterproof-iphone-ad-hoax-tricked-users-into-destroying-their-handsets. Luettu 24.11.2014.

Goldstein, S. 2014. Suburban Denver ‘swatting’ incident caught on gamer’s camera. New York Daily News. Luettavissa: http://www.nydailynews.com/news/national/suburban-denver-swatting-incident-caught-gamer-camera-article-1.1919640. Luettu 30.3.2015.

Griffiths, S. & Prigg, M. 2015. Microsoft kill Internet Explorer-Browser replaced Project Spartan. Daily Mail. Luettavissa: http://www.dailymail.co.uk/sciencetech/article-2999021/Microsoft-kill-Internet-Explorer-Browser-replaced-Project-Spartan.html. Luettu 25.3.2015.

Hacker News 2014. Anonymous headlines. Luettavissa: http://www.hackersnewsbulletin.com/category/anonymous-headlines. Luettu: 29.10.2014.

Henkilötietolaki 22.4.1999/523. Luettavissa: http://www.finlex.fi/fi/laki/ajantasa/1999/19990523. Luettu: 12.12.2014.

Indiegogo 2014. Anonabox: the Tor hardware router. Luettavissa: https://www.indiegogo.com/projects/anonabox-the-tor-hardware-router. Luettu:08.1.2015.

Internet Live Stats 2014. Luettavissa: http://www.internetlivestats.com/internet-users/. Luettu: 10.12.2014.

Jaeger, C. 2012. Deep Web Guides. Deep Enter the Dark Net. Luettavissa: http://www.deepwebguides.com/enter_the_dark_net.pdf. Luettu 31.3.2015.

Kroft, S. 2014. The Data Brokers: Selling your personal information. 60 Minutes. Luettavissa: http://www.cbsnews.com/news/the-data-brokers-selling-your-personal-information/. Luettu: 4.12.2014.

Laki yksityisyyden suojasta työelämässä 13.8.2004/759. Luettavissa: http://www.finlex.fi/fi/laki/ajantasa/2004/20040759. Luettu 12.12.2014.

Marketing-Schools 2012. Database Marketing. Luettavissa: http://www.marketing-schools.org/types-of-marketing/database-marketing.html. Luettu 9.12.2014.

Moon, M. 2014. Engadget Tor Browser vulnerability. Luettavissa: http://www.engadget.com/2014/11/18/tor-browser-vulnerability/. Luettu 22.1.2015.

Mozilla 2015a. Tietosuoja-, selaushistoria- ja seuranta-asetukset. Luettavissa: https://support.mozilla.org/fi/kb/tietosuoja-selaushistoria-ja-seuranta-asetukset. Luettu 11.3.2015.

Mozilla 2015b. Yksityinen selaus - Selaa verkkoa tallentamatta tietoja vierailemiltasi sivuilta. Luettavissa: https://support.mozilla.org/fi/kb/yksityinen-selaus-selaa-verkkoa-tallentamatta-tietoja. Luettu 14.4.2015.

Myall, S. 2014. Daily Mirror. Class A drugs by post from secret website: Sunday Mirror investigates. Luettavissa: http://www.mirror.co.uk/news/uk-news/class-drugs-post-secret-website-3604058. Luettu 30.3.2015.

Netmarketshare 2014. Operating system market share. Luettavissa: http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=8&qpcustomd=0. Luettu 4.11.2014.

Network advertising 2012. Understanding online adverstising. Luettavissa: http://www.networkadvertising.org/understanding-online-advertising. Luettu 9.12.2014.

Nissenbaum, H. 2014. The Meaning of Anonymity in an Information Age. Online Ethics Center. Luettavissa: http://www.onlineethics.org/cms/4675.aspx. Luettu: 2.12.2014.

No Bullying 2014. Amanda Todd Story. Luettavissa: http://nobullying.com/amanda-todd-story/. Luettu 21.1.2015.

National Security Agency. About NSA. Luettavissa. https://www.nsa.gov/about/faqs/about_nsa.shtml. Luettu 15.12.2014.

OkCupid 2014. Luettavissa: http://www.okcupid.com/legal/terms. Luettu 4.12.2014.

One Young World 2014. Luettavissa: http://www.oneyoungworld.com/blog/what-going-venezuela. Luettu: 2.12.2014.

Pagefair 2014. How adblocking is changing the web. Luettavissa: http://downloads.pagefair.com/reports/adblocking_goes_mainstream_2014_report.pdf. Luettu 10.12.2014.

Plussa 2014. Mikä on K-Plussa. Luettavissa: https://www.plussa.com/Mika-on-K-Plussa/ Luettu: 4.12.2014.

Reisinger, D 2015. Cnet. Silk Road 2.0's alleged 'DoctorClu' arrested on drug-related charges. Luettavissa: http://www.cnet.com/news/silk-road-2-0s-alleged-doctorclu-arrested-in-seattle-on-conspiracy-charges/. Luettu 22.1.2015.

Singer, N. 2012. Mapping, and Sharing, the Consumer Genome. New York Times. Luettavissa: http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html?_r=3&smid=tw-share. Luettu 3.12.2014.

Sonera 2012. Sonera toteutti Pirate Bay –estot. Luettavissa: http://uutishuone.sonera.fi/media/2012/07/30/sonera-toteutti-pirate-bay--estot/598baa16-a6c9-4660-855c-27e22a11fb7c. Luettu. 13.4.2015.

Sourander, A. Brunstein Klomek, A. Ikonen, M. Lindroos J. Luntamo T. Koskelainen M. Ristikari T. Helenius H. 2010. Psychosocial Risk Factors Associated With Cyberbullying Among Adolescents. American Medical Association. Luettavissa: http://archpsyc.jamanetwork.com/data/Journals/PSYCH/5298/yoa90114_720_728.pdf. Luettu: 19.11.2014.

Spiegel 2013. Luettavissa: http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html. Luettu 17.12.2014.

Sähköisen viestinnän tietosuojalaki 16.6.2004/516. Luettavissa: http://www.finlex.fi/fi/laki/ajantasa/2004/20040516. Luettu 12.12.2014.

Tails 2014. About. Luettavissa: https://tails.boum.org/about/index.en.html. Luettu 7.1.2015.

Tamblyn, T. 2014. iOS 8 'WAVE' Is Convincing People To Microwave Their iPhones. The Huffington Post. Luettavissa: http://www.huffingtonpost.co.uk/2014/09/22/ios-8-wave-hoax-iphone_n_5859728.html. Luettu 24.11.2014.

Tor Project 2014a. Overview. Luettavissa: https://www.torproject.org/about/overview.html.en. Luettu 17.12.2014.

Tor Project 2014b. Tor FAQ. Luettavissa: https://www.torproject.org/docs/faq.html.en#WhatIsTor. Luettu: 17.12.2014.

Tor Porject 2014c. Normal people use Tor. Luettavissa: https://www.torproject.org/about/torusers.html.en. Luettu 17.12.2014.

Tor Project 2014d. Tor: Sponsors. Luettavissa: https://www.torproject.org/about/sponsors.html.en. Luettu 17.12.2014.

Tor Project 2014e. Want Tor to really work? Luettavissa: https://www.torproject.org/download/download-easy.html.en. Luettu 7.1.2015.

Tor Project 2014f. A closer look at the Great Firewall of China. Luettavissa: https://blog.torproject.org/blog/closer-look-great-firewall-china. Luettu 7.1.2015.

Tor Project 2014g. Tor FAQ. Luettavissa: https://www.torproject.org/docs/faq#WhereDidVidaliaGo. Luettu: 7.1.2015.

Urban Dictionary. Trolling. Luettavissa: http://www.urbandictionary.com/define.php?term=trolling. Luettu 25.11.2014

Viestintävirasto 2014. Evästeet. Luettavissa: https://www.viestintavirasto.fi/kyberturvallisuus/palveluidenturvallinenkaytto/evasteet.html. Luettu 15.3.2014.

VPN Ground. VPN Service Explained -What is VPN Service & How does it work. Luettavissa: http://www.vpnground.com/blog/vpn-explained/. Luettu 17.4.2015.

Välimäki, M. 2004. Ideasta mediavaikuttajaksi. Luettavissa: http://www.valimaki.com/docs/effi_history.pdf. Luettu 2.12.2014.

Wisegeek 2014. What is a pseudonym. Luettavissa: http://www.wisegeek.com/what-is-a-pseudonym.htm. Luettu: 3.11.2014.

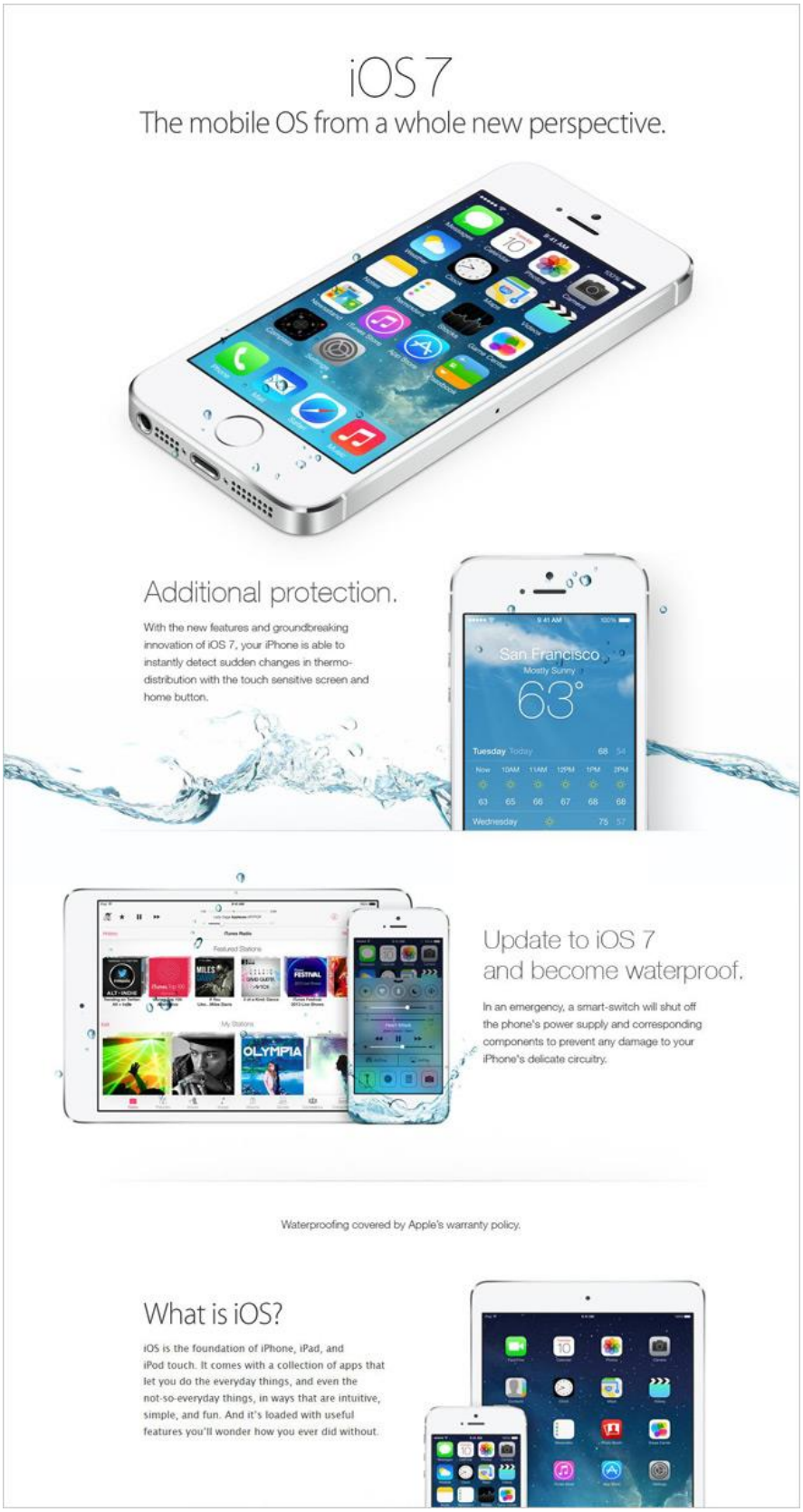
Yksityisyydensuoja 2014a. Anonyymit verkot. Luettavissa: https://www.yksityisyydensuoja.fi/content/anonyymit-verkot. Luettu 17.12.2014.

Yksityisyydensuoja 2014b. Lainsäädäntö. Luettavissa: https://www.yksityisyydensuoja.fi/lainsäädäntö. Luettu 10.11.2014.

Your Dictionary. Anonymity. Luettavissa: http://www.yourdictionary.com/anonymity. Luettu 29.10.2014.

Liitteet

Liite 1.

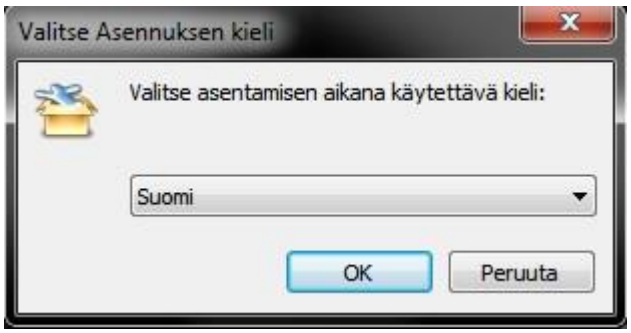


Kuva 1. 4chan foorumin iOS 7 mainoskampanja (Gibbs 2013)

Liite 2. Freenetin asentaminen

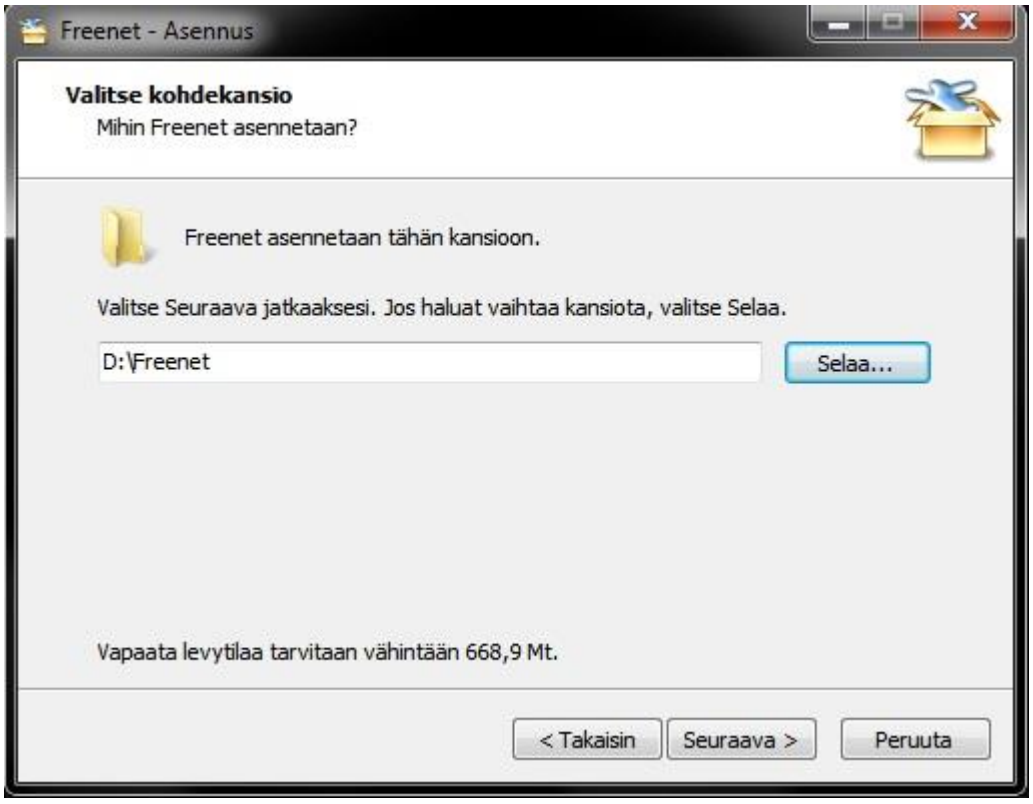
Freenetin asentamisen yhteydessä ei ilmennyt juuri mitään normaalista poikkeavaa ja aikaa siihen ei kulunut muutamaa minuuttia enempää.

Seuraavia kuvankaappauksia edeltävänä toimenpiteenä olen ladannut Freenet-projektin verkkosivuilta asennustiedoston, jonka suorittamisen seurauksena asennus prosessin ensimmäisenä vaiheena käyttäjän tulee valita haluttu asennuskieli (Kuva 2).



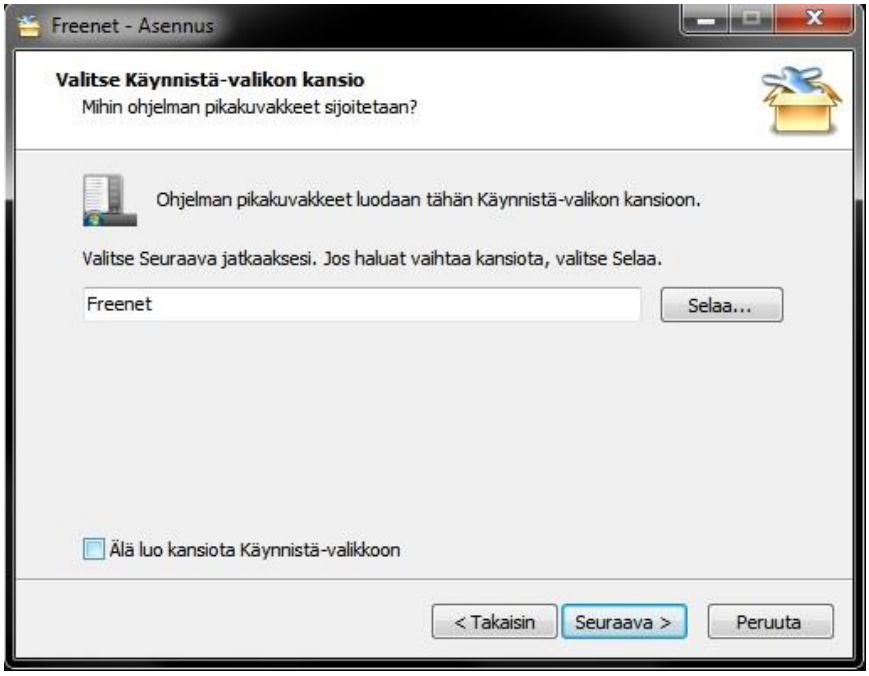
Kuva 2. Asennuskielen valinta

Tämän jälkeen vuorossa on kohdekansion valinta jota voi halutessaan lähteä muokkaamaan, mutta mikä ei kuitenkaan ole välttämätöntä (Kuva 3).



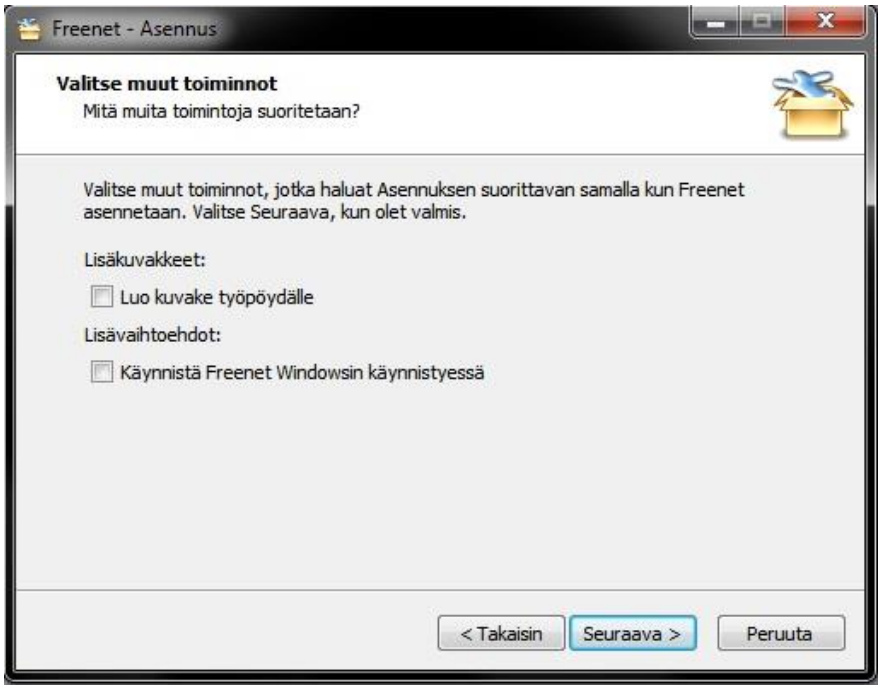
Kuva 3. Kohdekansion valinta

Asennuskielen ja kohdekansion valittuaan käyttäjän tulee vielä päättää haluaako tämä, että asennuksen yhteydessä ohjelmistolle luodaan oma uusi kansio Käynnistä-valikkoon (Kuva 4).



Kuva 4. Uuden kansion luominen Käynnistä-valikkoon

Halutessaan käyttäjällä on myös mahdollisuus luoda pikakuvake työpöydälle ja määritellä ohjelmisto käynnistämään automaattisesti tietokoneen käynnistyksen yhteydessä (Kuva 5).



Kuva 5. Muiden toimintojen valinta

Tämän jälkeen alkaa varsinaisesti itse asentaminen, joka on valmis hetkessä ja asennuksen loputtua käyttäjä voi halutessaan käynnistää Freenetin asennus-sovelluksen sulkemisen yhteydessä (Kuva 6.)

Kuva 6. Asennuksen viimeistely

Tämän jälkeen asennuksen on suoritettu ja vuorossa on Freenetin konfigurointien vuoro.

Liite 3

Alla olevissa taulukoissa on tarkemmin selostettuna, miten luvussa 7.1 mainitut historiatietoja koskevat määrittelyt vaikuttavat käytännössä Firefox-selaimen toimintaan. Taulukoissa käytetyt tiedot löytyvät Mozillan omilta verkkosivuilta.

Täydelliset historiatiedot
Mikäli selain on asetettu säilyttämään Täydelliset historiatiedot: - Firefox pitää yllä luetteloa vierailluista sivuista. - Luettelo ladatuista tiedostoista säilytetään Arkisto-ikkunassa. - Lomakekenttiin tai hakupalkkiin syötetty teksti säilytetään, jotta sitä pystytään käyttämään uudelleen. - Firefox hyväksyy evästeet verkkosivuilta kunnes ne vanhenevat. Halutessaan käyttäjällä on mahdollisuus poistaa evästeitä ja historiatietoja.

Taulukko 1. Ensimmäinen vaihtoehto, täydelliset historiatiedot (Mozilla 2015a)

Ei mitään historiatietoja
Mikäli asetukset on määritelty siten, ettei mitään historiatietoja säilytetä**:** - Firefox ei kirjaa selaushistoriaa. - Ladattuja tiedostoja ei luetteloida Arkisto-ikkunassa - Lomakekenttiin ja hakupalkkiin syötettyä tekstiä ei talleteta. - Firefox hyväksyy sivustojen evästeet ja poistaa ne, kun Firefox suljetaan. Vaihtoehto Ei mitään historiatietoja vastaa Firefoxin Yksityinen selaus -tilan käyttämistä. Napsauttamalla linkkiä poistaa kaikki kerätyt historiatiedot avautuu Poista historiatietoja -ikkuna, jossa voi nopeasti poistaa joitakin historiatietoja tai vaihtoehtoisesti kaikki historiatiedot.

Taulukko 2. Toinen vaihtoehto, ei mitään historiatietoja (Mozilla 2015a)

Valitut historiatiedot

Kun määritys puolestaan on Valitut historiatiedot, seuraavat asetukset ovat valittavissa:

- Selaa aina yksityinen selaus -tilassa**:**
  Kun tämä asetus on valittu, Firefox ei talleta mitään uusia historiatietoja, kun se seuraavan kerran käynnistetään.
- Säilytä selaushistoria ja tieto latauksista**:**
  Kun tämä asetus on valittu, Firefox tallettaa tiedon vierailluista sivuista ja ladatuista tiedostoista.
- Säilytä lomakkeiden ja hakupalkin tiedot**:**
  Kun tämä asetus on valittu, Firefox muistaa lomakekenttiin ja hakupalkkiin syötetyn tekstin, jolloin niitä voidaan käyttää uudelleen.
- Sivustot saavat asettaa evästeitä**:**
  Kun tämä asetus on valittu, Firefox hyväksyy sivustojen asettamat evästeet. Napsauttamalla painiketta Poikkeukset voi määritellä, mitkä sivustot saavat tai eivät saa asettaa evästeitä.
- Salli kolmannen osapuolen evästeet**:**
  - Aina: Firefox hyväksyy kaikki evästeet sivustolta http://sivusto2.com kun vieraillaan sivustolla http://sivusto1.com.
  - Vierailluilta sivustoilta**:** Jos sivustolla http://sivusto2.com on vierailtu aikaisemmin, Firefox hyväksyy sen evästeet myös vierailtaessa sivustolla http://sivusto1.com, muussa tapauksessa Firefox ei hyväksy evästeitä.
  - Ei milloinkaan**:** Firefox ei koskaan hyväksy evästeitä sivustolta
- Säilytä evästeet**:**
  - kunnes ne vanhenevat**:** Kun tämä vaihtoehto on valittu, Firefox antaa vierailtujen sivustojen määrittää itse, kuinka kauan niiden evästeitä säilytetään.
  - kunnes Firefox suljetaan**:** Kun tämä vaihtoehto on valittu, Firefox poistaa kaikki evästeet aina, kun se suljetaan.
  - kysy aina erikseen**:** Kun tämä vaihtoehto on valittu, ja sivusto yrittää asettaa evästettä, Firefox kysyy joka kerta erikseen, kuinka kauan sitä säilytetään.

  - Poista historiatiedot, kun Firefox suljetaan:
    Valitut tallennetut tiedot poistetaan, kun Firefox suljetaan. Napsauttamalla painiketta Asetukset avautuu ikkuna, jossa voi valita poistettavat tiedot.

Taulukko 3. Kolmas vaihtoehto, täydelliset historiatiedot (Mozilla 2015a)